AXIOMTEK

IFW320

Industrial Firewall Appliance

User's Manual

Disclaimers

This manual has been carefully checked and believed to contain accurate information. Axiomtek Co., Ltd. assumes no responsibility for any infringements of patents or any third party's rights, and any liability arising from such use.

Axiomtek does not warrant or assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information in this document. Axiomtek does not make any commitment to update the information in this manual.

Axiomtek reserves the right to change or revise this document and/or product at any time without notice.

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Axiomtek Co., Ltd.

Trademarks Acknowledgments

Axiomtek is a trademark of Axiomtek Co., Ltd.

Windows® is a trademark of Microsoft Corporation.

Other brand names and trademarks are the properties and registered brands of their respective owners.

©Copyright 2015 Axiomtek Co., Ltd.

All Rights Reserved

January 2015, Version A1

Printed in Taiwan

Safety Precautions

Before getting started, please read the following important safety precautions.

1. Be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and place all electronic components in any static-shielded devices. Most electronic components are sensitive to static electrical charge.

2. Disconnect the power cord from the IFW320 Series before making any installation. Be sure both the system and the external devices are turned OFF. Sudden surge of power could ruin sensitive components. Make sure the IFW320 Series is properly grounded.

3. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.

4. Turn OFF the system power before cleaning. Clean the system using a cloth only. Do not spray any liquid cleaner directly onto the screen.

5. Do not leave this equipment in an uncontrolled environment where the storage temperature is below -45°C or above 85°C. It may damage the equipment.

6. Do not open the system's back cover. If opening the cover for maintenance is a must, only a trained technician is allowed to do so. Integrated circuits on computer boards are sensitive to static electricity. To avoid damaging chips from electrostatic discharge, observe the following precautions:

    - Before handling a board or integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. This will help to discharge any static electricity on your body.
    - When handling boards and components, wear a wrist-grounding strap, available from most electronic component stores.

Classification

1. Degree of production against electric shock: Not classified

2. Degree of protection against the ingress of water: IPX0

3. Equipment not suitable for use in the presence of a flammable anesthetic mixture with air or with oxygen or nitrous oxide.

4. Mode of operation: Continuous

5. Type of protection against electric shock: Class I equipment

General Cleaning Tips

You may need the following precautions before you begin to clean the computer. When you clean any single part or component for the computer, please read and understand the details below fully.

When you need to clean the device, please rub it with a piece of dry cloth.

1. Be cautious of the tiny removable components when you use a vacuum cleaner to absorb the dirt on the floor.

2. Turn the system off before you start to clean up the component or computer.

3. Never drop the components inside the computer or get circuit board damp or wet.

4. Be cautious of all kinds of cleaning solvents or chemicals when you use it for the sake of cleaning. Some individuals may be allergic to the ingredients.

5. Try not to put any food, drink or cigarette around the computer.

Cleaning Tools:

Although many companies have created products to help improve the process of cleaning your computer and peripherals, users can also use household items to clean their computers and peripherals. Below is a listing of items you may need or want to use while cleaning your computer or computer peripherals.

Keep in mind that some components in your computer may only be able to be cleaned using a product designed for cleaning that component, if this is the case it will be mentioned in the cleaning.

- Cloth: A piece of cloth is the best tool to use when rubbing up a component. Although paper towels or tissues can be used on most hardware as well, we still recommend you to rub it with a piece of cloth.
- Water or rubbing alcohol: You may moisten a piece of cloth a bit with some water or rubbing alcohol and rub it on the computer. Unknown solvents may be harmful to the plastics parts.
- Vacuum cleaner: Absorb the dust, dirt, hair, cigarette particles, and other particles out of a computer can be one of the best methods of cleaning a computer. Over time these items can restrict the airflow in a computer and cause circuitry to corrode.
- Cotton swabs: Cotton swaps moistened with rubbing alcohol or water are excellent tools for wiping hard to reach areas in your keyboard, mouse, and other locations.
- Foam swabs: Whenever possible it is better to use lint free swabs such as foam swabs.

Note

It is strongly recommended that you should shut down the system before you start to clean any single components.

Please follow the steps below:

1. Close all application programs.
2. Close operating software.
3. Turn off power switch.
4. Remove all devices.
5. Pull out power cable.

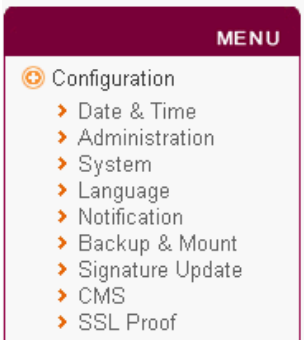
Scrap Computer Recycling

If the computer equipments need the maintenance or are beyond repair, we strongly recommended that you should inform your Axiomtek distributor as soon as possible for the suitable solution. For the computers that are no longer useful or no longer working well, please contact your Axiomtek distributor for recycling and we will make the proper arrangement.

Conventions Used in This Manual

The following typographical conventions are used in this book:

Content Style
Menu > Submenu > Right Side Banner Selections
e.g. *Configuration > Administrator > System Setup*



To make sure that you perform certain tasks properly, take note of the following symbols used throughout this manual.

Note — This icon indicates a tip, or suggestion. I would like to tell users a special point on the Internet.

Caution — This icon indicates a limited or caution. Pay attention to these to avoid running into system.

Example — This icon indicates an example. Give users examples and to show how to use.

Table of Contents

Disclaimers ii
Safety Precautions iii
Classification iv
General Cleaning Tips iv
Cleaning Tools: v
Scrap Computer Recycling v
Conventions Used in This Manual vi

Chapter 1 Introduction 1

1.1 Features 1
1.2 Specifications 2
1.3 I/O Outlets 5
1.4 DIN Rail Mounting 6

Chapter 2 Getting Started 7

2.1 Basic System Configuration 7
2.1.1 Connect to Hardware and Software 7
2.1.2 Account and Password Default Setting 7
2.1.3 Default Language 8
2.2 Starting Machine Up 8
2.2.1 LAN 9
2.2.2 WAN 10
2.3 Homepage Information 12
2.3.1 Menu Bar 12
2.3.2 MENU 12
2.3.3 System Time and System Resource 12
2.3.4 System Information and Server Service 12
2.3.5 Administrator Login 13
2.3.6 Interface 13

Chapter 3 Configuration 15

3.1 Date & Time 15
3.1.1 Setting 16
3.2 Administration 17
3.2.1 Administrator 17
3.2.2 System 19
3.2.3 IP Address 21

3.2.4 Clear Data 21
3.2.5 SMTP Server 22
3.3 System 25
3.3.1 System Backup 25
3.3.2 Schedule Backup 25
3.3.3 Firmware Upgrade 26
3.4 Language 27
3.5 Notification 27
3.5.1 Notification 27
3.5.2 Log 28
3.6 Backup & Mount 30
3.6.1 Data Backup 30
3.6.2 Data Mount 31
3.7 Signature Update 32
3.7.1 Signature Update 32
3.8 CMS 32
3.8.1 CMS Setting 33
3.9 SSL Proof 34
3.9.1 SSL Proof Set 35
Chapter 4 Network 37
4.1 Interface 37
4.1.1 LAN 39
4.1.2 WAN 42
4.2 Interface (IPv6) 44
4.2.1 LAN 44
4.2.2 WAN 45
4.2.3 DNS Server 45
4.3 Routing 46
4.3.1 Routing Table 46
4.3.2 Dynamic Routing 47
4.3.3 IPv6 Routing Table 47
4.4 802.1Q 48
4.4.1 802.1Q 48
Chapter 5 Policy 53
5.1 LAN Policy and WAN Policy 53
Chapter 6 Objects 57
6.1 Address Table 57
6.1.1 LAN IP Address 57

6.1.2 LAN Group 58
6.1.3 WAN IP Address 61
6.1.4 WAN Group 62
6.2 Services 62
6.2.1 Basic Service 62
6.2.2 Service Group 63
6.3 Schedule 65
6.3.1 Schedule List 65
6.4 QoS 67
6.4.1 QoS Setting 67
6.5 Application Control 69
6.5.1 Setting 69
6.6 URL Filter 72
6.6.1 List Settings 73
6.6.2 URL Settings 74
6.6.3 Other Settings 75
6.7 Virtual Server 76
6.7.1 Virtual Server 76
6.7.2 Mapped IP 79
6.8 Firewall Protection 80
6.8.1 Firewall Protection 80
6.8.2 Attack Log 81
6.9 Authentication 81
6.9.1 Auth Setting 82
6.9.2 Local User 84
6.9.3 POP3, RADIUS User 85
6.9.4 User Group 87
6.9.5 AD User 92
6.9.6 Log 92
6.9.7 Status 93
6.10 Bulletin Board 93
6.10.1 Bulletin Setting 94
6.10.2 Has Read the Bulletin Board 97

Chapter 7 Network Services 99

7.1 DHCP 99
7.1.1 LAN User List 99
7.1.2 LAN DHCP Server 100
7.1.3 DHCP Static IP 100
7.2 DDNS 101
7.2.1 DDNS Server 101
7.3 DNS Proxy 102

7.3.1 General Setting 103
7.4 High Availability 103
7.4.1 High Availability 103
7.5 SNMP 109
7.5.1 SNMP 109
7.6 Remote Syslog Server 110
7.6.1 Remote Connect Setup 110

Chapter 8 Advanced Protection 117

8.1 Anomaly IP Analysis 117
8.1.1 Log Anomaly 117
8.1.2 Notify Anomaly 118
8.1.3 Block Anomaly 120
8.1.4 Trusted IP 121
8.1.5 Anomaly Log 121
8.1.6 Block List 122
8.2 Switch Management 122
8.2.1 Switch Setup 122
8.3 Internal Protection 125
8.3.1 Spoofing Setup 125
8.3.2 ARP Spoofing Log 126
8.3.3 MAC Collision Log 127
8.3.4 IP Collision Log 127
8.3.5 Lock Status 128

Chapter 9 IDP & BotNet 129

9.1 IDP Setting 129
9.1.1 Basic Setting 129
9.2 IDP Log 131
9.2.1 IDP Log 131
9.2.2 IDP Log Search 131
9.3 BotNet Setting 133
9.3.1 Operation Mode 135
9.3.2 BotNet Filter Setting 135
9.4 BotNet Log 136
9.4.1 Today BotNet Log 136
9.4.2 BotNet Log Search 137

Chapter 10 SSL VPN 139

10.1 SSL VPN Setting 140
10.1.1 SSL VPN Setup 140
10.1.2 SSL Client List 141

10.2 SSL VPN Log 145
10.2.1 SSL Client On-Line Log 145
10.3 VPN Policy 145

Chapter 11 VPN 147

11.1 IPSec Tunnel 147
11.1.1 IPSec Tunnel 147
11.1.2 Add IPSec Tunnel 151
11.2 PPTP Server 151
11.2.1 PPTP Server 152
11.2.2 Add Account 153
11.2.3 PPTP Account List 154
11.3 PPTP Client 155
11.3.1 Add PPTP Client 155
11.3.2 PPTP Client List 155
11.4 VPN Policy 156
11.4.1 Internal to VPN and VPN to Internal 156

Chapter 12 Tools 159

12.1 Connection Test 159
12.1.1 Ping 159
12.1.2 Traceroute 160
12.1.3 DNS Query 161
12.1.4 Port Scan 161
12.1.5 IP Route 164
12.1.6 Interface Information 165
12.1.7 Wake Up 166
12.2 Remote Management 167

Chapter 13 Logs 169

13.1 System Operation 169
13.1.1 Logs 169
13.1.2 Logs Search 170
13.1.3 Logs Search Result 171

Chapter 14 Status 173

14.1 Performance 173
14.1.1 System Status 173
14.1.2 Interface Flow 174
14.1.3 History Status 175
14.2 Connection Status 176
14.2.1 Computer List 176

14.2.2 Connection Track 176
14.3 Flow Analysis 178
14.3.1 Top N Flow 178
14.3.2 Top N Port Flow 179
14.3.3 Top N Search 180

Chapter 1 Introduction

Industrial automation industries adopt TCP/IP protocol to simplify development and maintenance. However, this exposes equipment to cyber attacks, and malware. The IFW320 comes with Firewall and VPN features, making it an ideal choice for industrial firewall appliance. It is also suitable for Ethernet security application in sensitive remote control or monitoring networks, such as in oil, gas, water & wastewater, power or factory automation system.

Equipped with stateful packet inspection, Denial of Service (DoS), and Intrusion Detection & Prevention (IDP) features, the Firewall appliance could be used to protect machine and equipment connecting to un-trusted Internet. Built in with IPSec VPN that provides site to site secure tunnel, PPTP VPN that offers point to point connection for employee at home, and SSL VPN that offers you an easy VPN access to your headquarters simply through a web browser, the Firewall device provide system integrator and machine maker a secure way to configure and maintain their device.

The Firewall appliance also have Industrial Protocol management including EtherCAT, Ethernet/IP, Lonworks, Profinet, Modbus, DNP that pave a way to secure fieldbus network. Additionally, we offer wide temperature models for use in hazardous -40°C~75°C environments, and economic-friendly model 0~60°C for non-temperature-sensitive use.

1.1 Features

- All-in-one Firewall/NAT/VPN
- Security protection: Firewall, IDP, BotNet
- Secure connection: VPN, SSL VPN, WAN connection checking
- IPv4/IPv6 dual mode
- Easy network setup with Network Address Translation (NAT)
- Quick installation, USB restore
- Centralized management
- Wide operation temperature: -40°C~75°C (IFW320-T)

1.2 Specifications

Software

- **Interface**
  - LAN: 1 RJ-45 port.
  - WAN: 1 RJ-45 port.

- **Network Features**
  - Quality of Service QoS.
  - Support IPv4/IPv6.

- **Routing**
  - Static routing, RIP v1/v2.

- **Firewall Features**
  - Stateful inspection.
  - Filter: MAC, IP, port, protocol.
  - Bridge mode firewall.
  - Denial of Service DoS protection: TCP(SYN), ICMP(ping), ARP(Bridge mode), Port scan.
  - NAT: 1-1 NAT, Port forwarding.
  - Application software management: VoIP, P2P, SMS, Web, Web Mail and Entertainment software.
  - Industrial Protocol management: EtherCAT, Ethernet/IP, Lonworks, Profinet, Modbus, DNP.
  - URL white list.
  - Virtual server.
  - System status: system performance, connecting status, data flow analysis.
  - Whitelist: user group, existing IP white list.
  - Router/Firewall Redundancy.

- **Intrusion Detection and Prevention**
  - IDP (Intrusion Detection and Prevention).
  - BotNet prevention.
  - Abnormal IP analysis.
  - Switch management.

- **VPN Features**
  - Protocol: IPSec, PPTP, SSL VPN.
  - Encryption: DES, 3DES, AES.
  - Authentication: Pre-Shared Key(PSK), SHA, MD5.
  - IPSec Dead Peer Detection.
  - Show remote Network Neighborhood.
  - SSL VPN: server setting, certificate setting.
  - SSL concurrent VPN channels: Max. 50.
  - SSL VPN user number: Max. 300.
  - VPN channel number:
    - IPSec channels: Max. 100.
    - PPTP client: Max. 50.
    - PPTP server: Max. 50.
  - VPN control.
  - Stateful packet inspection.
  - NAT Traversal.

- **Data Throughput**
  - 500Mbps.

- **VPN Throughput**
  - 3Des: 50Mbps.
  - Des: 78Mbps.
  - Aes:: 85Mbps.

- **Management**
  - Support Network Time Protocol NTP.
  - Web management: HTTP, HTTPS.
  - System file backup and upgrade.
  - Interface (WAN/LAN) flow statistics.
  - System configuration: system configuration default restoration, message notification, export/import.
  - Network Service: Routing table, 802.1Q, DDNS, DNS proxy, SNMP, DHCP client/server.
  - Centralized Management System CMS client/server.
  - Networking test:
    - Ping, Traceroute, DNS Query, Server Link.
    - IP route.
    - Interface Information, Wake Up, IPv6.

Hardware

- **Standard Color**
  - Silver-Black.

- **Construction**
  - Extruded aluminum and heavy-duty steel, IP40.

- **CPU**
  - Intel Atom processor E3815 (1.4GHz).

- **System I/O Outlet**
  - VGA: One DB15 connector.
  - USB: One USB 2.0.
  - LAN: Two 1000/100/10 Ethernet ports.
  - Magnetic isolation protection: 1.5KV.
  - Power input: One DC power input with terminal block.

- **Memory/Storage**
  - 2GB DRAM, 2GB CompactFlash.

- **System Indicator**
  - System: Power, Ready/Active.

- **Power Supply**
  - Wide range 12VDC~24VDC power input with terminal block.
  - DC version: OVP, UVP, Reverse protection.

- **Operating Temperature**
  - 0°C~60°C (IFW320).
  - -40°C~75°C (IFW320-T).

- **Storage Temperature**
  - -40°C~85°C.

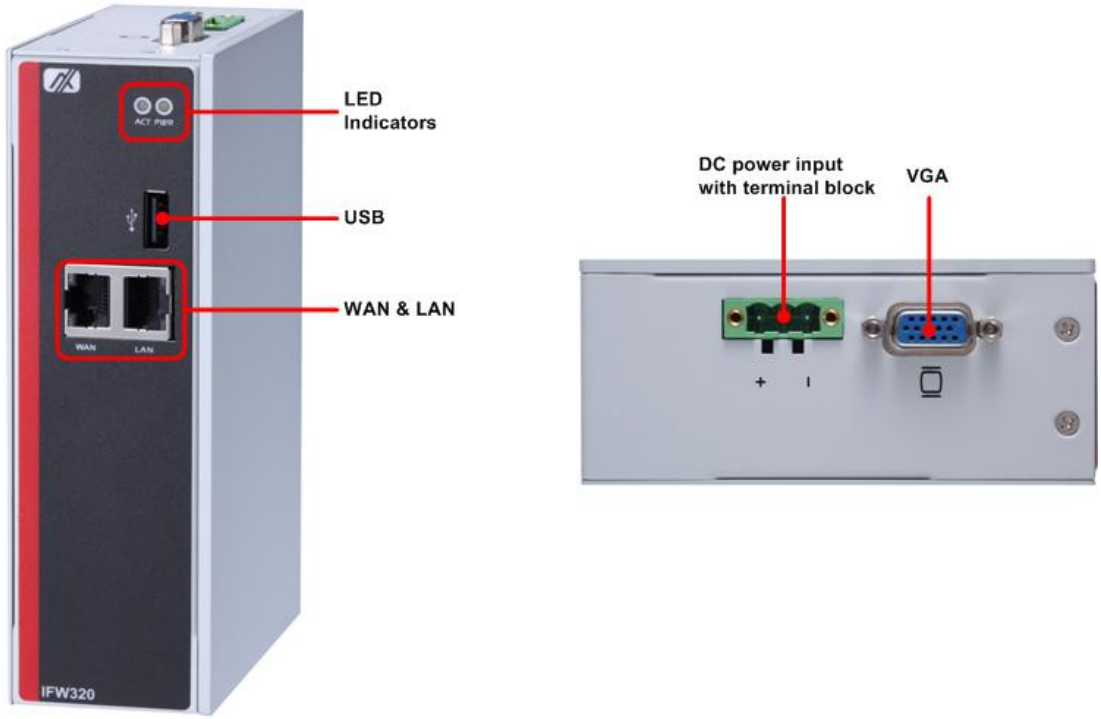
- **Humidity**
  - 10%~95%.
- **Vibration Endurance**
  - 2G@5~500Hz, Amplitude 0.35mm (operation/storage/transport).
- **Weight**
  - 1kg.
- **Certification**
  - CE.
  - FCC Part 18.
  - UL60950-1 (compliance).
- **Dimensions**
  - 48 x 110 x 155mm.

Note

All specifications and images are subject to change without notice.

1.3 I/O Outlets

The following figures show I/O outlets on front view and top view of the IFW320.

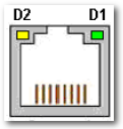


- **ACT LED:** Indicate the storage status and it flashes when system is accessing data from the storage.
- **PWR LED:** Indicate the Power status. When the DC input is acceptable, the LED will ON.
- **USB:** USB 2.0 port.
- **WAN Port:** Connect to the perimeter router
- **LAN Port:** Connect to the Intranet of the company.
- **Terminal Block:** DC power input with terminal block.
- **VGA:** VGA port for console.

Note

Description of Gigabit LAN/WAN connector is indicated in table below.

D2: Link/Activity LED		*D1: Bi-color Speed LED*	
Status	***Description***	***Status***	***Description***
Green	*Link*	*Off*	*10Mbps*
Blinking	*Activity*	*Green*	*100Mbps*
		Yellow	*1000Mbps*

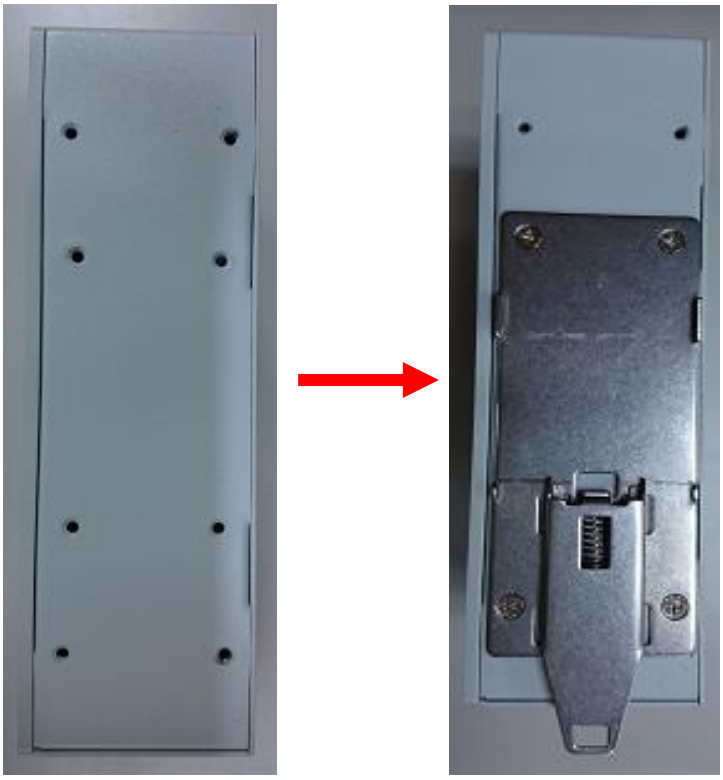


1.4 DIN Rail Mounting

The IFW320 provides DIN rail mounting kit for user to mount the system to a standard DIN rail. Follow steps below:

1. Prepare components for DIN rail mounting, screws and bracket.

2. Fasten the bracket to the system with screws firmly.



Chapter 2
Getting Started

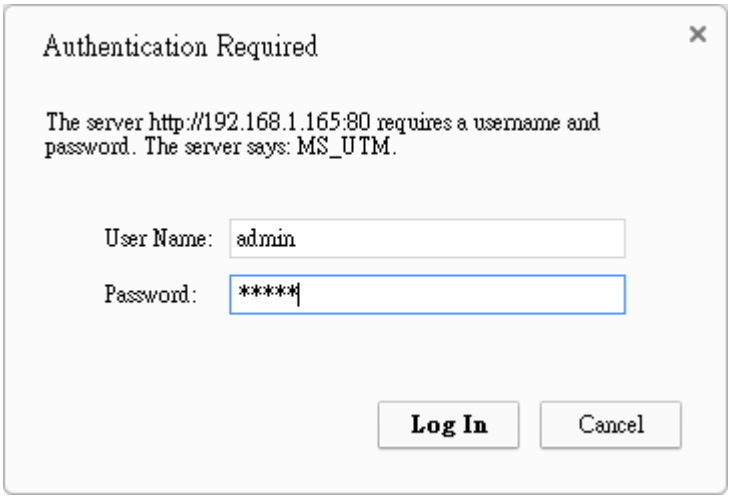
2.1 Basic System Configuration

2.1.1 Connect to Hardware and Software

Connect both the IT administrator's PC and the device's LAN port to the same hub/switch, and launch a web browser (e.g. Internet Explorer or Mozilla Firefox) to access the management interface address which is set to *http://192.168.1.1* by default. Therefore, the IP addresses of LAN PCs must be configured within the range between 192.168.1.2 and 192.168.1.254 inclusively, and assigned the subnet mask of 255.255.255.0.

2.1.2 Account and Password Default Setting

You will be prompted for the user name and password when accessing the management interface, see figure below.



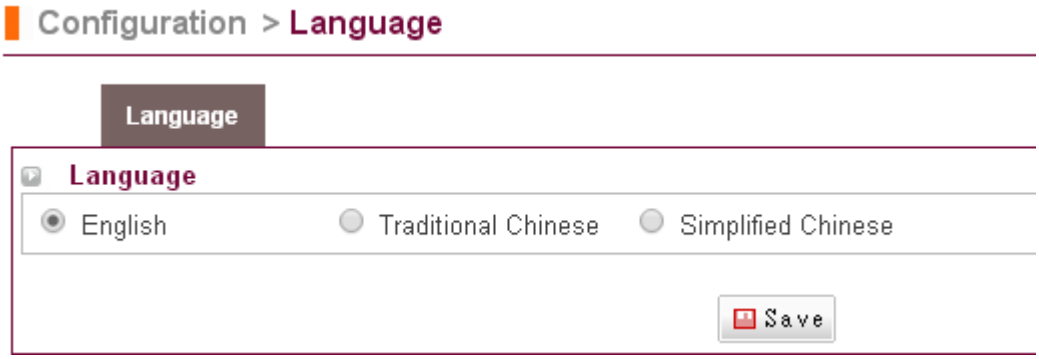
Account
Default setting is "admin".

Password
Default setting is "admin".

Click Log In.

2.1.3 Default Language

The default language for management interface is English. Select *Configuration* > *Language* > *Language*. Then, there are three languages: English, Traditional Chinese and Simplified Chinese. Select one language which belongs to you. Click on Save.



2.2 Starting Machine Up

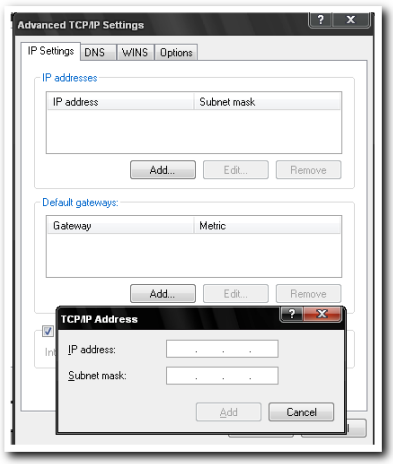
In this section, we provide LAN setup and WAN setup configurations for starting machine up.

Note

When you want to configure a new LAN interface address, please do: if the company's LAN IP address does not belong to subnet of 192.168.1.0/24 (default), the Administrator must add/change PC IP address to be within the same range of the LAN subnet.

Example

For example, here is how to add multiple IP address (192.168.1.2) in LAN connection with your Windows operating system.

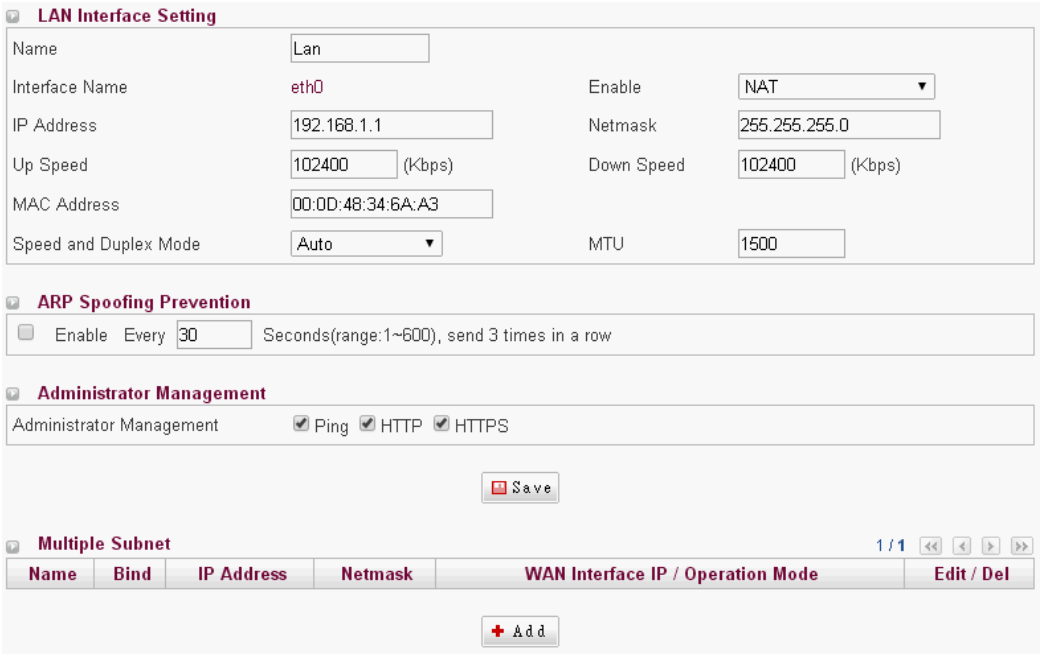


Caution

For your reference, please configure your management address based on the available subnet ranges: 10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255 or 192.168.0.0~192.168.255.255.

2.2.1 LAN

Select *Network* > *Interface* > *LAN*, see figure below.



Name
Enter a name that you remember easily.

IP Address
Enter a new IP address. Default setting is 192.168.1.1.

Up Speed (Up Speed = Upstream Bandwidth)
The Kbps is a unit of Speed. Define a suitable maximum Upstream bandwidth in order that the device may use it as a basis for operating. If Up Speed of LAN interface is 100M, it can be setup to 102400Kbps. Therefore, 1Gbps will be setup to 1024000Kbps.

MAC address
Enter a MAC address.

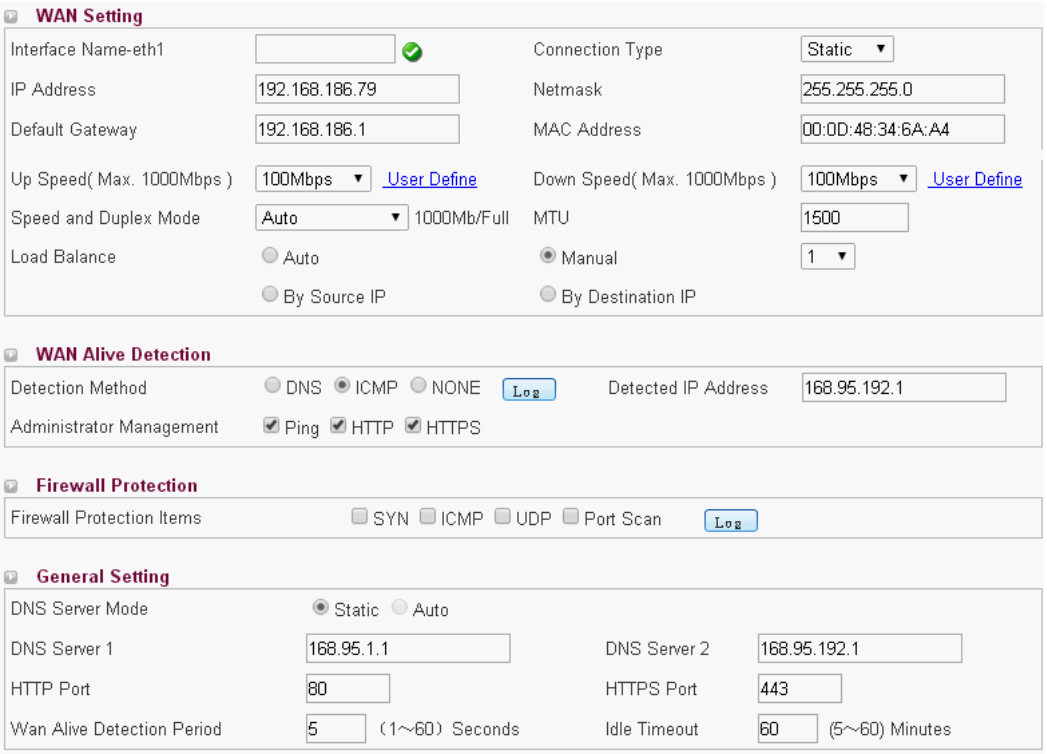
Netmask
Enter a new Netmask. Default setting is 255.255.255.0.

Down Speed (Down Speed = Downstream Bandwidth)
The Kbps is a unit of Speed. Define a suitable maximum Downstream bandwidth in order that the device may use it as a basis for operating. If Down Speed of LAN interface is 100M, it can be setup to 102400Kbps. Therefore, 1Gbps will be setup to 1024000Kbps.

After click on Save, please enter a new IP address that you have just made in web browser and then login again.

2.2.2 WAN

Select *Network* > *Interface* > *WAN*, see figure below.



Interface Name-eth1
Enter any word for recognition.

IP Address
Depend on the Connection Method. DHCP and PPPoE mode do not need to set IP address. Only Static mode needs to setup IP address.

Default Gateway
Depend on the Connection Method. DHCP and PPPoE mode do not need to set Default Gateway. Only Static mode needs to setup Default Gateway.

Up Speed (Max. 1000Mbps)
The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on Custom Define link to set your speed according to ISP's WAN Speed.

Speed and Duplex Mode
Usually, it sets on Auto. You also can select other settings.

Load Balancing
It offers four methods:

1. Auto: Distributes the outward sessions by the usage status of each WAN port.
2. By Source IP: For services that require using the same IP address throughout the process, such as online game and banking, IFW320 helps user retain the same WAN port (i.e. IP address) over which the session was created to avoid disconnection caused by the variation of the user's IP address.
3. Manual: According to administrator demand for sharing loading on the WAN.
4. By Destination IP: Once a session is created between the IFW320 and a specific host, then the following sessions linking to that host will be automatically distributed to the same WAN port.

Connection Method
There are three Connection methods.
1. Static: Static IP address.
2. DHCP: Using DHCP to get IP address from ISP.
3. PPPoE: PPPoE.

Netmask
Enter a Netmask. Default setting is 255.255.255.0.

MAC address
Enter a MAC Address.

Down Speed
The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on User Define link to set your speed according to ISP's WAN Speed.

Check Method
Using DNS, ICMP or NONE to check whether WAN is on or off. Both DNS and ICMP need to setup IP address for test.
1. DNS: Tests the validity of Internet connection by requesting the domain name.
2. ICMP: Uses ping command to test the validity of Internet connection.
3. NONE: Line is not detected; the connection status is always on line.

Management Service
There are three multiple-choice modes, PING, HTTP, and HTTPS. In addition, you can click Log to see more detail recorder.
1. Ping: The network can be detected by Ping commands when ticked
2. HTTP: The management interface is available for accessing via HTTP Protocol when ticked.
3. HTTPS: The management interface is available for accessing via HTTPS Protocol when ticked.

Firewall Protect Items
There are four multiple-choice, SYN, ICMP, UDP, and Port Scan. It offers currently available protection. In addition, you can click on Log to see more detail recorder.

DNS Server 1
The IP address of the DNS server used for the bulk of DNS lookups. Default setting is 168.95.1.1.

HTTP Port
HTTP port number for management. Default setting is 80.

WAN Check Time
System administrators can enter the system every interval of time to do more testing, unit is calculated in seconds. Default setting is 3 second.

DNS Server 2
The IP address of the backup DNS server. Use it when the Primary DNS server is unreachable. Default setting is 168.95.192.1.

HTTPS Port
HTTPS port number for management. Default setting is 443.

Disconnect if idle for
The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection. The minute is a unit of time. Default setting is 60 minutes.

2.3 Homepage Information

2.3.1 Menu Bar

Through menu bar, on top of the screen, you can know different models depend on the different colors.

2.3.2 MENU

On the other hand, through MENU (from the left side of the screen), you can see different function lists depend on the different models. UR model has Content Recorder function, but it does not have IDP and SSL VPN functions. AW model has IDP and SSL VPN function, but it does not have Content Recorder function.

2.3.3 System Time and System Resource

It shows Server 1-1 Date & Time, Current Time zone. It also displays the CPU, Memory, Flash, and HDD simultaneously from 9-1 Performance. See figure below.

System Time		
Server Date / Time	2014-11-10	17:37:30
Current Timezone	Asia/Taipei	
Server Uptime	10 days,2 hours,43 minutes	

System Resource	
System Loading	0.00 0.02 0.12
CPU Loading	1.0%
RAM (1 GB)	28%
Flash (1,146 MB)	8%

2.3.4 System Information and Server Service

The Server Model and Server Version of the machine, see figure below.

1. : Service works.
2. : Service does not work.

Server Info	
Server Model	IFW320
Server Version	6.1.9
Machine's Number	1418900111

Server Service	
DHCP Services	
DDNS Services	
IPSec VPN Service	
HA	

2.3.5 Administrator Login

The administrator log in name, IP address, the number of people login in the meantime, also how long it takes to automatically renew the home page news. Or establish the time in which the system automatically renew; in every three, five, ten, 20, 30 seconds.

2.3.6 Interface

Equipment Interface details, see figure below.

Interfaces » More			
Name		LAN	WAN
Interface		eth0	eth1
Connect Status			
Line Status			
IP Address		192.168.1.1	192.168.186.79
Total Packets	Tx	5,941	362,486
	Rx	31,872	1,650,785
Total Flow (byte)	Tx	1.40M	59.84M
	Rx	3.67M	143.93M

Name
The system catches network contact surface name.

Connect Status
Indicate whether the network is unimpeded.

1. : Connect up.
2. : It does not connect the Internet.

Line Status
Whether the judgment network does connect

1. : Connect up.
2. : It does not connect the Internet.

IP Address
System binding IP address

Total Packets
Each network interface transmission, receive wrapped packets quantity (in bytes).

Total Flow
Each network interface transmission, receive current capacity (in bytes).

This page is intentionally left blank.

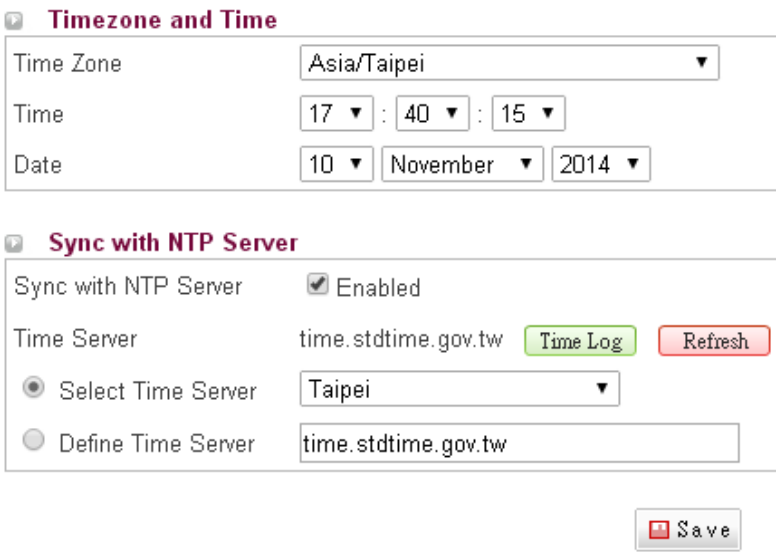
Chapter 3
Configuration

In this chapter, you may learn how to configure Date Time, Administrator, Backup, Upgrade, and Language of your machine by enabling the following lists:

- Date & Time
- Administration
- System
- Language
- Notification
- Backup & Mount
- Signature Update
- CMS
- SSL Proof

3.1 Date & Time

Your current time zone setting can also be changed in this section. The first form in this section gives you the possibility to manually change the system time. Second, the system time synchronized to time server hosts on the Internet by using the network time protocol (NTP = Network Time Protocol). A number of time server hosts on the Internet are preconfigured and used by the system. This makes sense if the system clock is way off and you would like to speed up synchronization. Finally, this might be necessary if you are running a setup that does not allow Axiomtek to reach the Internet. You can add a host on User Defined Time Server field. In the Date & Time section you can enable the following lists (see figure below):



3.1.1 Setting

Select *Configuration* > *Date & Time* > *Setting*. There are two parts: Timezone and time and Network Time Retrieval.

Method 1: Synchronize to the local computer, see figure below.

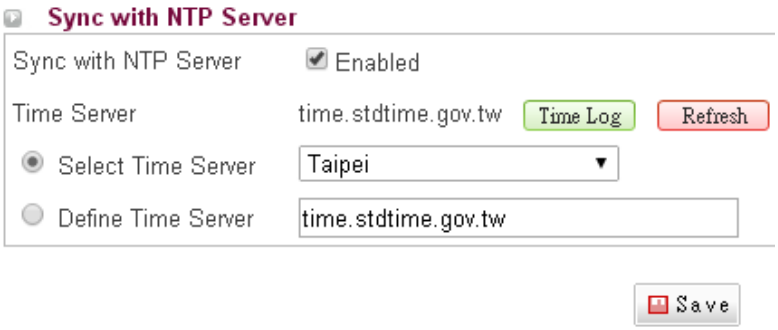
Time Zone
Select your country time zone.

Time
Select the local time.

Date
Select the local date.

Click on Save.

Method 2: The date and time settings can be configured by either synchronizing to an Internet Network Time Server.



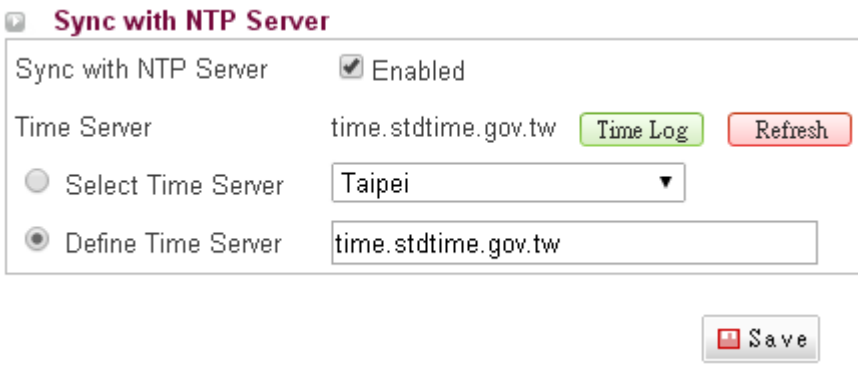
Sync with NTP Server
Select “Enabled” in Network Time Retrieval.

Selected Time Server
Select your country time server.

Click Refresh
Click on Time Log to check time log information, and it keeps within three days log information.

Click on Save**.**

Method 3: This might be necessary if you are running a setup that does not allow Axiomtek to reach the Internet.



Sync with NTP Server
Select Enabled in Network Time Retrieval.

User Defined Time Server
Enter a time server you know.

Click on Refresh.
Click on Time Log to check time log information, and it keeps within three days log information.

Click on Save.

3.2 Administration

This section mainly explains the authorization settings for accessing. It covers the subjects of Administrator Setup, System Setup, Manage IP Address, Clear Data, and SMTP Server Setting. In this section you can enable the following lists:

3.2.1 Administrator

Select *Configuration* > *Administration* > *Administrator*. The default account and password are both "admin". IT administrator can create several sub-administrators with different permission and menu customization. In addition, default "admin" is permitted to use all privileges and all menus, such as the privileges of packets that pass through the equipment and monitoring controls. "Admin" (system manager) can manage monitor and configure setting of functions. Some sub-administrations (account) are set to "Read", it is "read-only" and is not able to change any setting of the machine.

Account
Enter account name.

Password
The password for authentication.

Password Strength

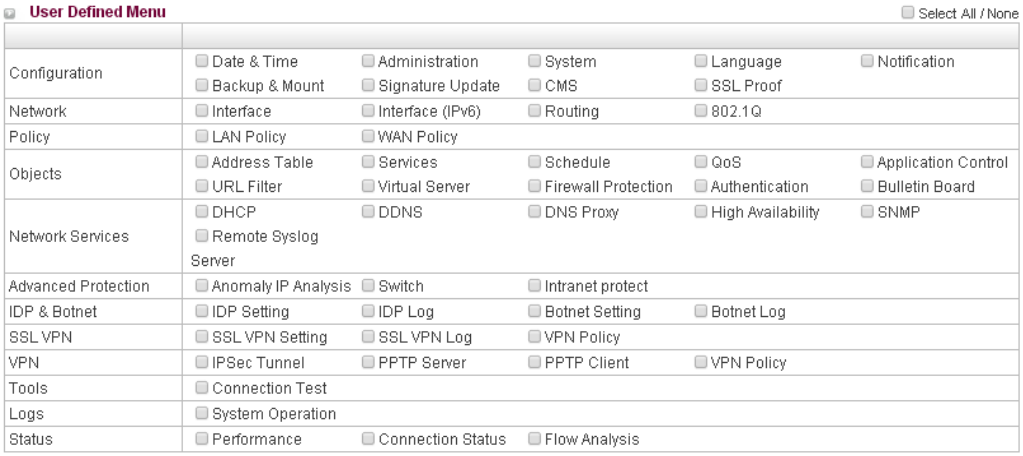
Password
(Please input 3 to 16 characters, not the same with account)
Password Strength
Weak Fair Strong
Password
(Please input 3 to 16 characters, not the same with account)
Password Strength
Weak Fair Strong
Password
(Please input 3 to 16 characters, not the same with account)
Password Strength
Weak Fair Strong

Confirm Password
The confirmation of password

Notes
Easy to know who it is.

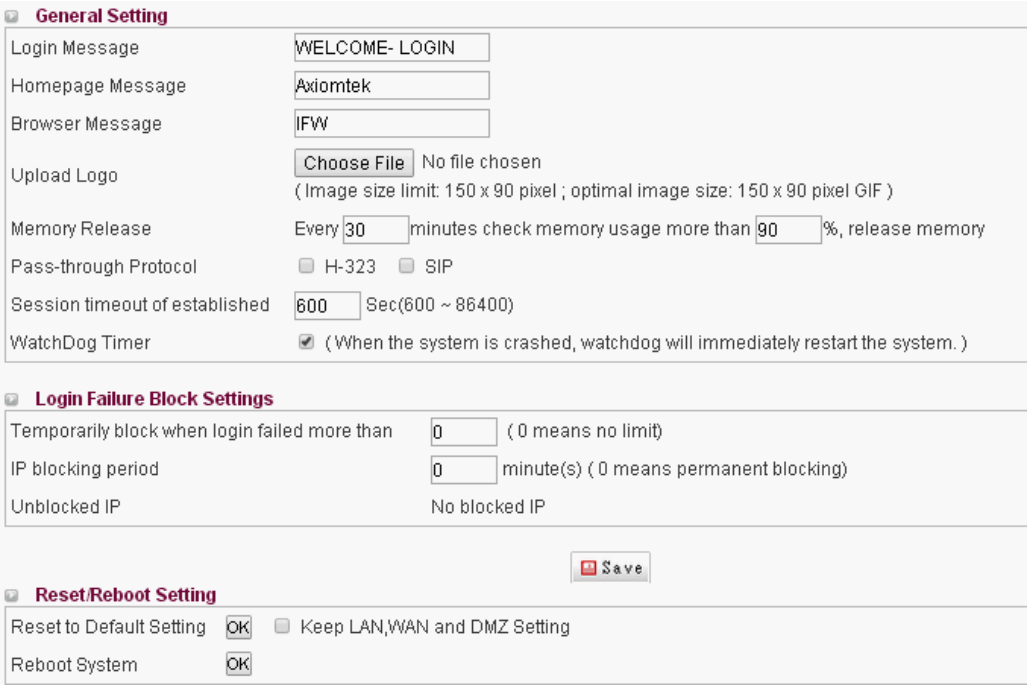
Privilege
Sub-administrators can be granted with Read, Write, or All Privileges to determine the right of system. Besides, sub-administrators can be created, edited or deleted.

User Defined Menu
IT administrator could customize MENU by selecting, see figure below.



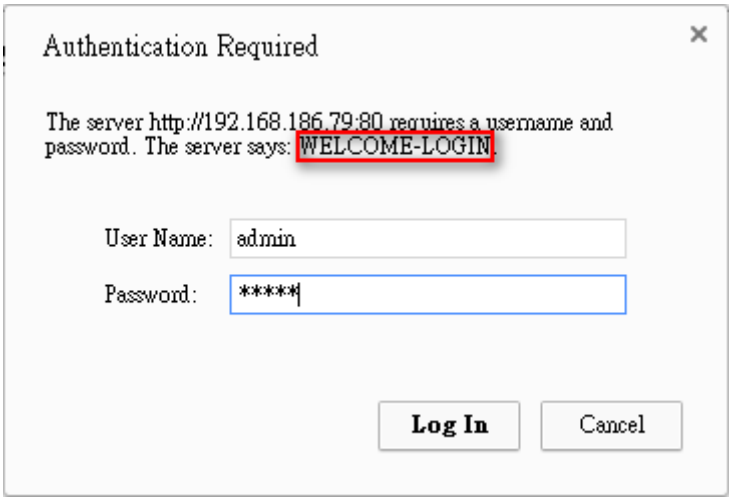
3.2.2 System

Select *Configuration* > *Administration* > *System*. This function shows view of the screen and system default setting, see figure below.



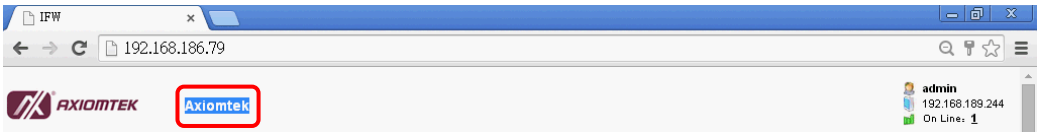
Login Title

Enter a name, and then click on Sure. The name you enter will be showed when you login.

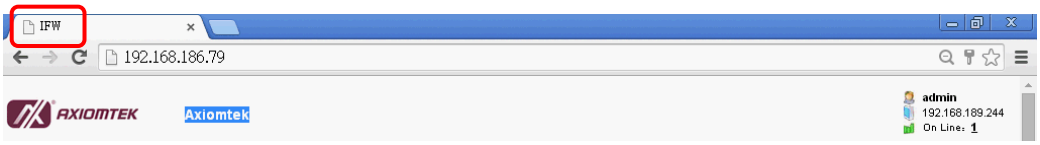


Menu Bar Title

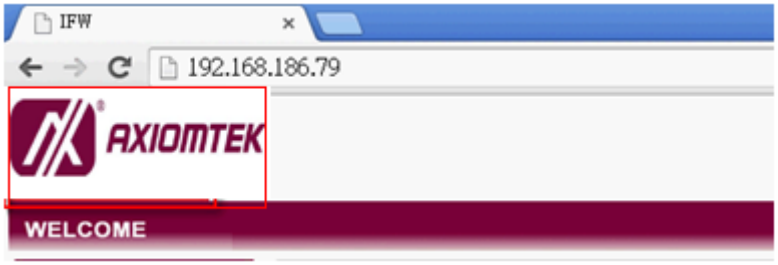
Enter a name, and then click on Sure. The name you enter will be showed next to the logo picture.



Browser Title
Enter a name, and then click on Sure. The name you enter will be showed on the top of browser.



Change Logo
Click on Browse... to upload resolution of 150x90 gif figure file, and then click on Save. The image will automatically appear in the upper left corner of the screen.



Memory Release
How often the system checks memory. When memory usage is up to the setting value (%), system will release memory if it has high memory usage. (Please see memory status in Homepage Information.)

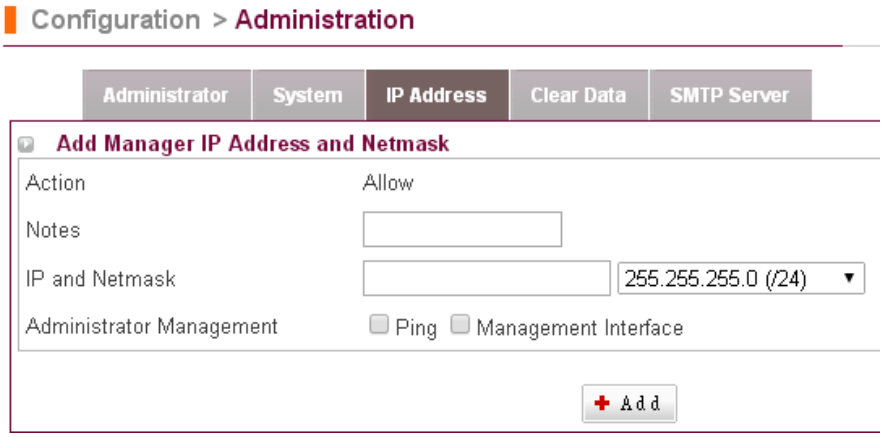
Protocol Pass-Through
System supports H-323 and SIP.

Reset to Default Setting
If you need to keep LAN and WAN IP setting, please select the related check box. If you do not select, it means that you want to reset to default setting.

Reboot system
Click on reboot to reboot system.

3.2.3 IP Address

Select *Configuration* > *Administration* > *IP Address*. Click on Add to create a new management IP and Netmask. In order for this Manager IP Address option to be effective, the IT administrator must cancel the ping, HTTP and HTTPS selections in WAN Setup. Then, the management WAN interface will be inaccessible. Moreover, all systems are granted access with the correct password if no administrative IP addresses or networks are specified.

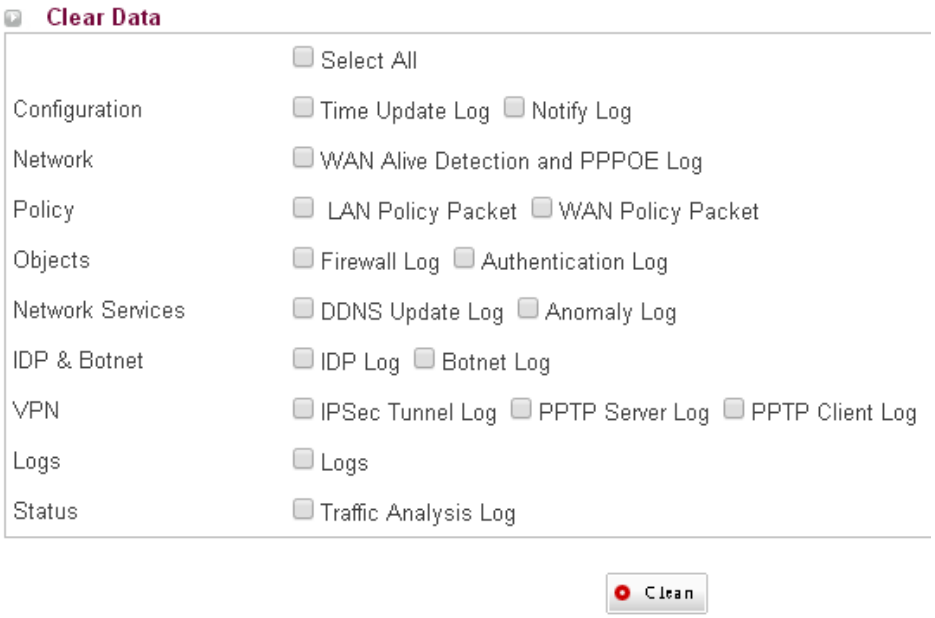


Note
Enter any word for recognition.

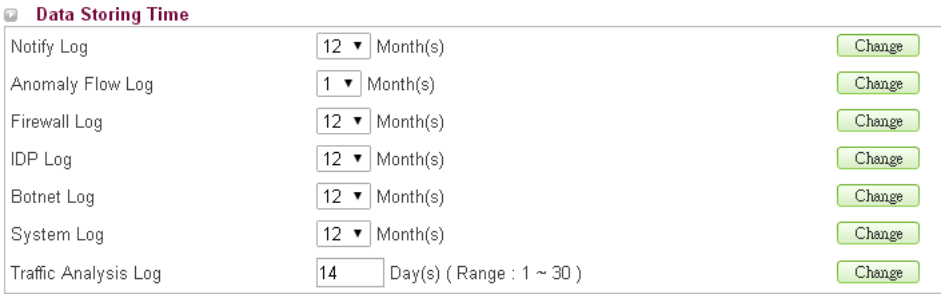
IP and Netmask
It accords with WAN Setup which selects Networking from the MENU on the left side of the screen, and then selects Interface from the submenu. Then, click WAN; you will see WAN Alive Check below.

3.2.4 Clear Data

Select *Configuration* > *Administration* > *Clear Data.* There are two parts: Clear Data and Data Storing Time.



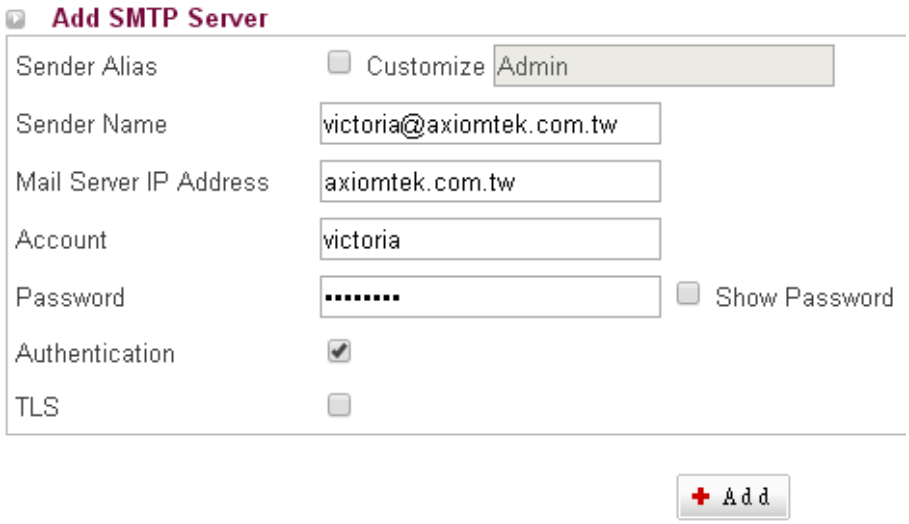
Clear Data
In order to clear more spaces of hard disk, delete some records and logs which are not necessary by clicking on Clean. It is also possible to check all connections by clicking on the Select All pane.



Data Storing Time
Select numbers. Otherwise, enter how many days you want to keep logs. Click Change buttons if you modify numbers.

3.2.5 SMTP Server

Select *Configuration* > *Administration* > *SMTP Server.*



Sender Name
Enter your SMTP account or user name.

Mail Server IP Address
Enter SMTP server address.

Account
Enter your SMTP account or user name.

Password
Enter account password.

Authentication
Select it if your SMTP server needs an authentication to connect to.

TLS
Select it if your SMTP server used TLS protocol.

Delivery Domain Name
If Delivery Domain Name is the same as the domain of receiver, the email will be sent from this SMTP setting; if not, the email will be sent from the first SMTP setting.

Click on

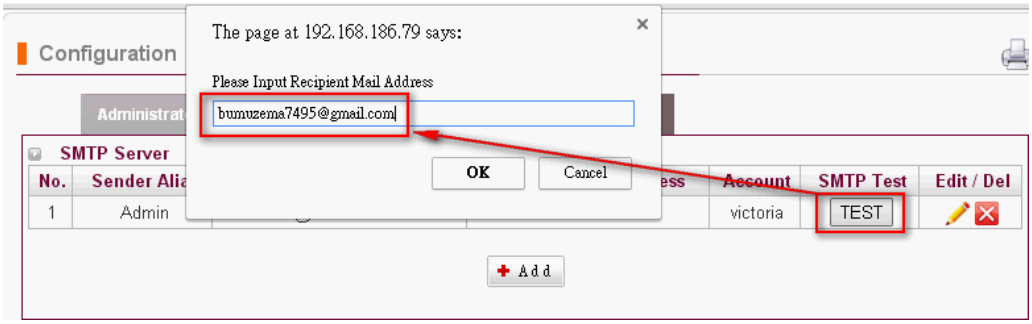
Setting SMTP Server completed. In addition, click on

to create a new sub-SMTP. to modify its contents, or to cancel list.

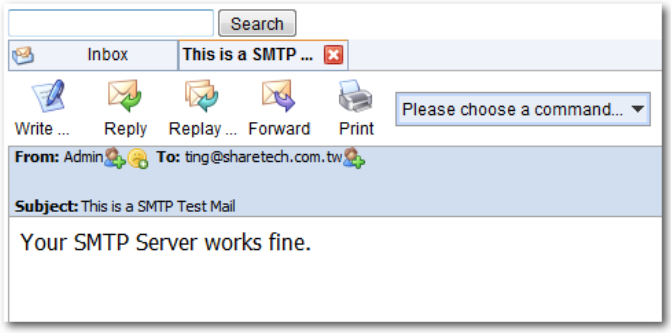
Click on

To test whether your SMTP is fine or not, please click on

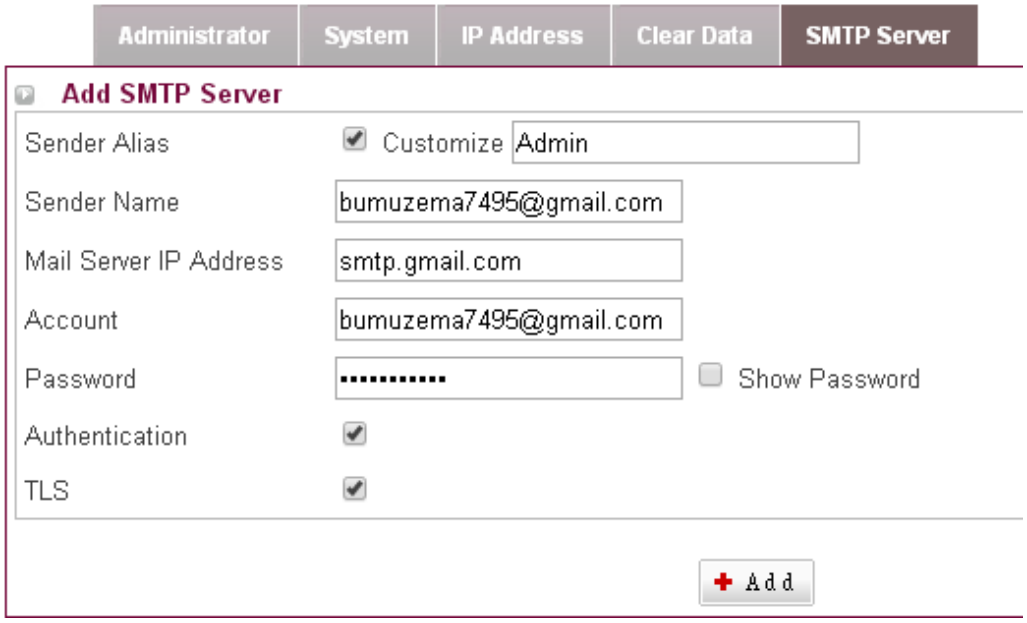
, see figure below.



If users got email as below, your setting is correct. Otherwise, user has to check user's SMTP server setting again.



Or you can also create other SMTP servers to get your notifications information. For instance, you can use Gmail SMTP server as below.



Setting SMTP Server completed. In addition, click on

to create a new sub-SMTP. to modify its contents, or to cancel list.

3.3 System

In this section you can enable the following lists:

3.3.1 System Backup

Select *Configuration* > *System* > *System Backup.* Then you will see two parts: System Backup and System Recovery.

System Backup (to USB)

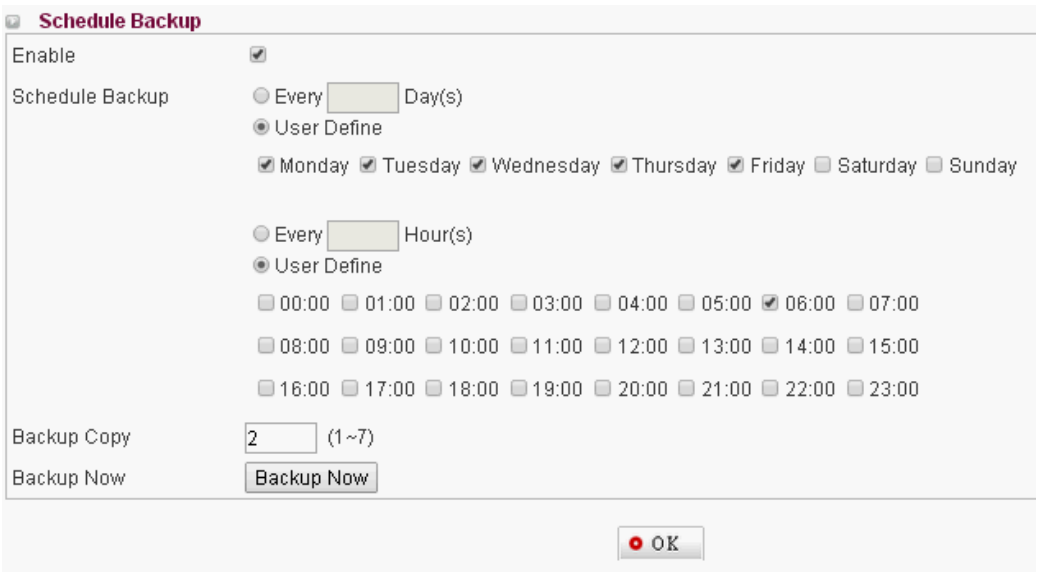
Click on Backup, and then please wait a minute. You will see another window. Click on OK, and do not forget where you save file.

System Recovery

Click on Browse..., and then select the file. After you select the file, do not forget to click on OK on the screen.

3.3.2 Schedule Backup

Select *Configuration* > *System* > *Schedule Backup.* As long as IT administrators enable backup, setup time and copies, the system will provide scheduled backup.



Enable
Check to enable schedule backup.

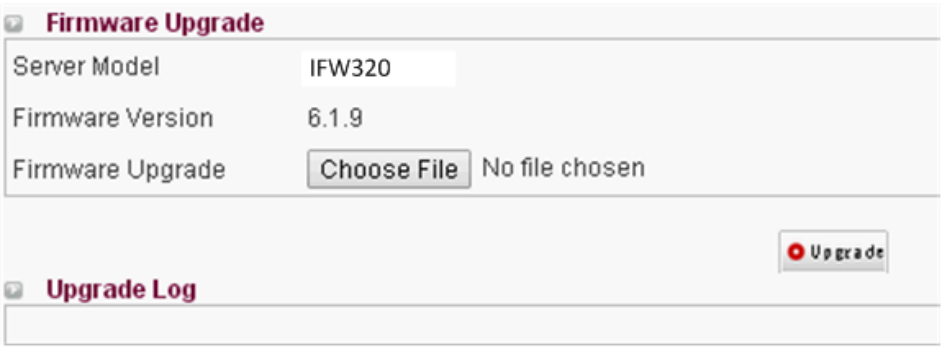
Schedule Backup
Check to choose backup time. You may choose to back up every day(s) or check on user define to select your backup times.

Backup Copy
The default is “1” copy.

Backup Now
Click on Backup Now to back up immediately.

3.3.3 Firmware Upgrade

Select *Configuration* > *System* > *Firmware Upgrade.* Then you will see two parts: Software Upgrade and Upgrade Record.



Server Model
It displays model name.

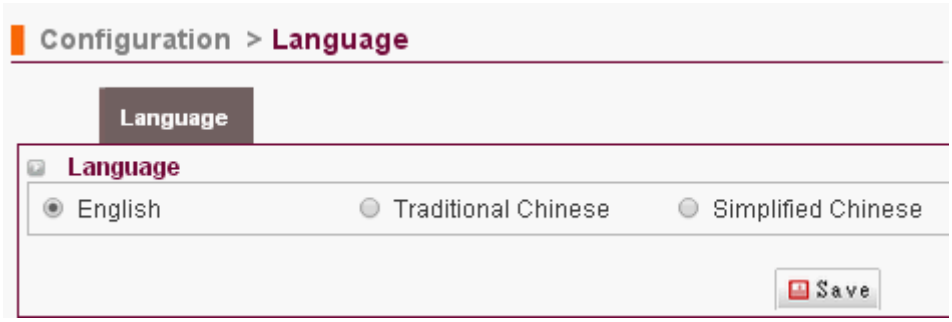
Firmware Version
It displays current software version.

Firmware Upgrade
You could know information about server model and current software version.

Upgrade Log
It shows all of upgrade information you had done before.

3.4 Language

Select *Configuration* > *Language* > *Language*. It offers three languages for you to select: English, Traditional Chinese, and Simplified Chinese. Select a language which belongs to you.

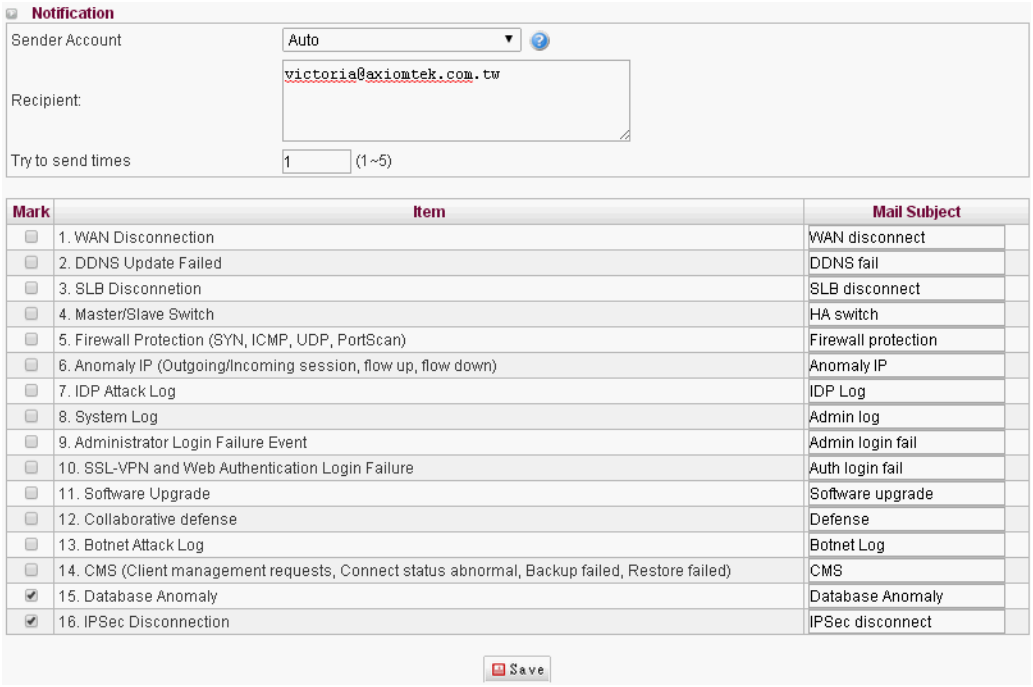


3.5 Notification

This function is useful for reminding users when exceptions occur. In this section you can enable the following lists:

3.5.1 Notification

Select *Configuration* > *Notification* > *Notification.*



Sender Account
Default selection is "Auto." Select one SMTP server which you have ever set in *Configuration* > *Administration* > *SMTP Server*.

Current Setting
After users select SMTP Setting, system will shows current SMTP server setting automatically.

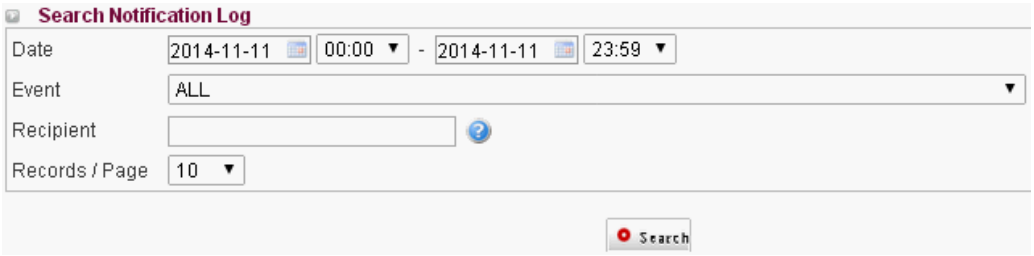
Recipient
Enter receiver email addresses.

Click on

Click this to save settings you made.

3.5.2 Log

Select *Configuration > Notification > Log.*



Date
Set date and time.

Event
Set information that you want to search.

Recipient
The mail receiver.

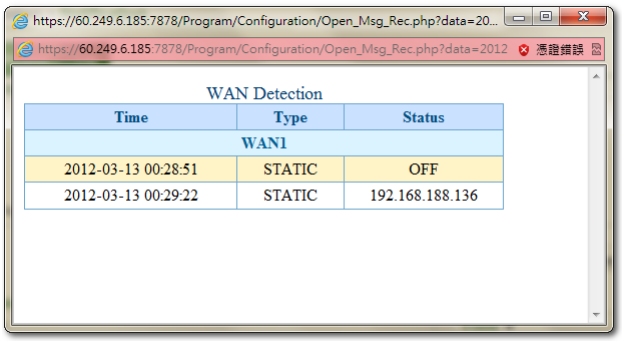
Records / Page
Select how many data would be shown on the screen.

Click on

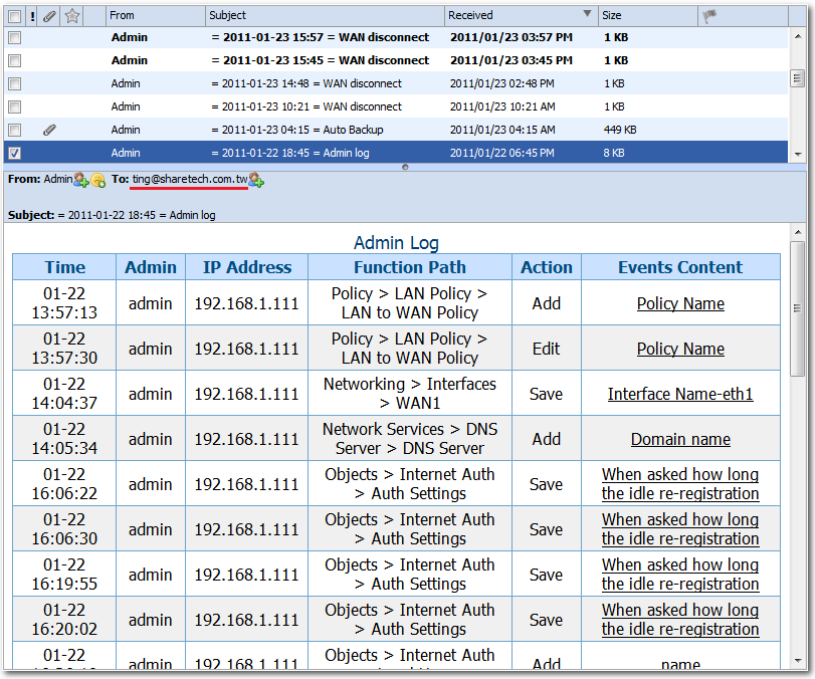
After you click on

, you will see the result on the screen.

Click on to see logs.



Recipients would get emails, see figures below.



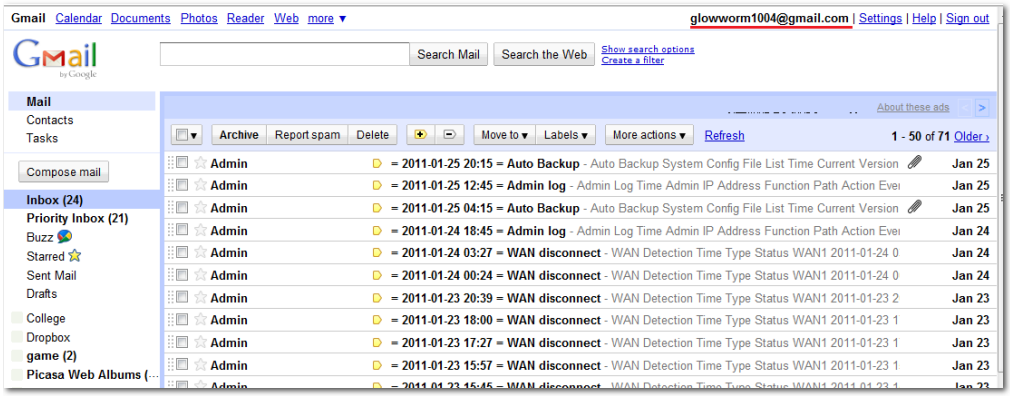
From	Subject	Received	Size
Admin	**= 2011-01-23 15:57 = WAN disconnect**	**2011/01/23 03:57 PM**	**1 KB**
Admin	**= 2011-01-23 15:45 = WAN disconnect**	**2011/01/23 03:45 PM**	**1 KB**
Admin	= 2011-01-23 14:48 = WAN disconnect	2011/01/23 02:48 PM	1 KB
Admin	= 2011-01-23 10:21 = WAN disconnect	2011/01/23 10:21 AM	1 KB
Admin	= 2011-01-23 04:15 = Auto Backup	2011/01/23 04:15 AM	449 KB
Admin	= 2011-01-22 18:45 = Admin log	2011/01/22 06:45 PM	8 KB

From: Admin **To:** ting@sharetech.com.tw

Subject: = 2011-01-22 18:45 = Admin log

Admin Log

Time	Admin	IP Address	Function Path	Action	Events Content
01-22 13:57:13	admin	192.168.1.111	Policy > LAN Policy > LAN to WAN Policy	Add	Policy Name
01-22 13:57:30	admin	192.168.1.111	Policy > LAN Policy > LAN to WAN Policy	Edit	Policy Name
01-22 14:04:37	admin	192.168.1.111	Networking > Interfaces > WAN1	Save	Interface Name-eth1
01-22 14:05:34	admin	192.168.1.111	Network Services > DNS Server > DNS Server	Add	Domain name
01-22 16:06:22	admin	192.168.1.111	Objects > Internet Auth > Auth Settings	Save	When asked how long the idle re-registration
01-22 16:06:30	admin	192.168.1.111	Objects > Internet Auth > Auth Settings	Save	When asked how long the idle re-registration
01-22 16:19:55	admin	192.168.1.111	Objects > Internet Auth > Auth Settings	Save	When asked how long the idle re-registration
01-22 16:20:02	admin	192.168.1.111	Objects > Internet Auth > Auth Settings	Save	When asked how long the idle re-registration
01-22	admin	192.168.1.111	Objects > Internet Auth	Add	name



Gmail Calendar Documents Photos Reader Web more ▾ glowworm1004@gmail.com | Settings | Help | Sign out

Search Mail | Search the Web | Show search options | Create a filter

Mail | Contacts | Tasks

Compose mail

Inbox (24) | Priority Inbox (21) | Buzz | Starred | Sent Mail | Drafts | College | Dropbox | game (2) | Picasa Web Albums (...

Archive | Report spam | Delete | Move to ▾ | Labels ▾ | More actions ▾ | Refresh | 1 - 50 of 71 Older ›

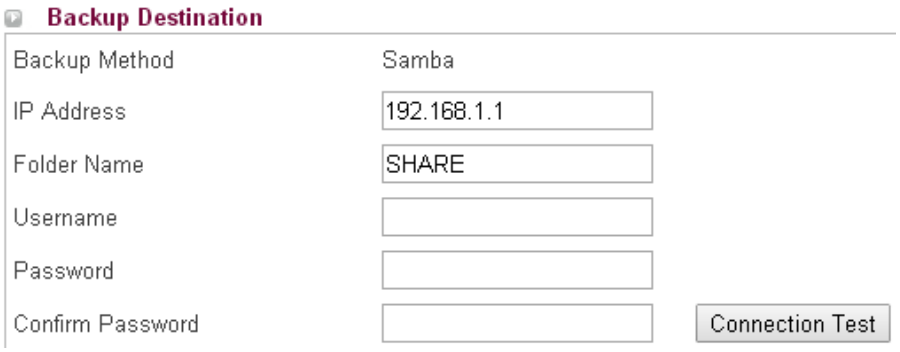
Admin	= 2011-01-25 20:15 = Auto Backup - Auto Backup System Config File List Time Current Version	Jan 25
Admin	= 2011-01-25 12:45 = Admin log - Admin Log Time Admin IP Address Function Path Action Ever	Jan 25
Admin	= 2011-01-25 04:15 = Auto Backup - Auto Backup System Config File List Time Current Version	Jan 25
Admin	= 2011-01-24 18:45 = Admin log - Admin Log Time Admin IP Address Function Path Action Ever	Jan 24
Admin	= 2011-01-24 03:27 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-24 0	Jan 24
Admin	= 2011-01-24 00:24 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-24 0	Jan 24
Admin	= 2011-01-23 20:39 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-23 2	Jan 23
Admin	= 2011-01-23 18:00 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-23 1	Jan 23
Admin	= 2011-01-23 17:27 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-23 1	Jan 23
Admin	= 2011-01-23 15:57 = WAN disconnect - WAN Detection Time Type Status WAN1 2011-01-23 1	Jan 23

3.6 Backup & Mount

Some IT administrators get into huge trouble when IFW320's hard disk is broken, and the worse, IT administrators do not backup system as scheduled or users forget where those files are. Moreover, users may also come across insufficient storage available problem. Therefore, users would like this function in order to schedule data backup automatically.

3.6.1 Data Backup

Select *Configuration* > *Backup & Mount* > *Data Backup.*



Backup Method
Samba

IP Address
Enter an IP address.

Folder Name
Enter a folder name you like.

Caution ***User has to create this folder name in C: drive if your OS is Windows.***

Username
Enter username here.

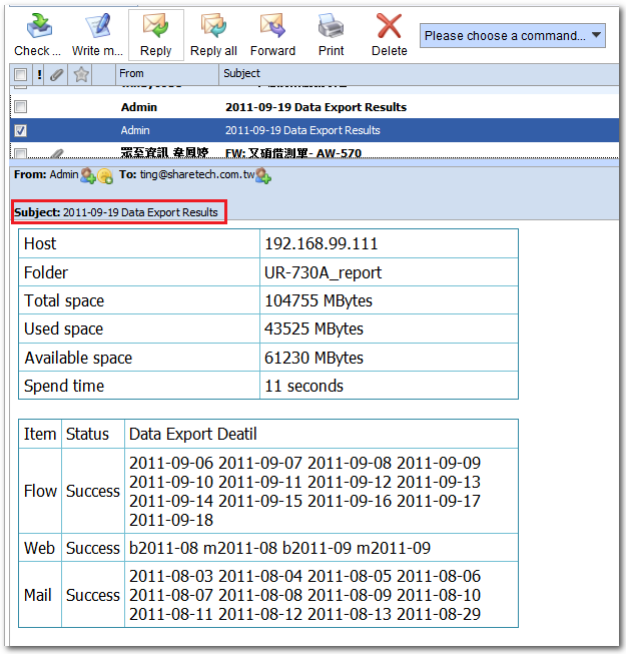
Password
Enter user password here.

Confirm Password
Password confirmation.

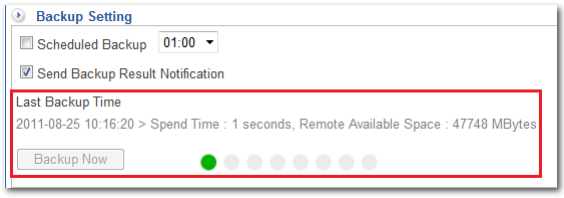
Click on Connection Test
You will see the message below if your setting is correct.

Scheduled Backup
Select the time you want the system to run backup schedule.

Send Backup Result Notification
User have to go to *Configuration* > *Notification* > *Notification* to set your information first. Then, you will get mail after system backup successfully.



Click on Backup Now
You will see the following message.

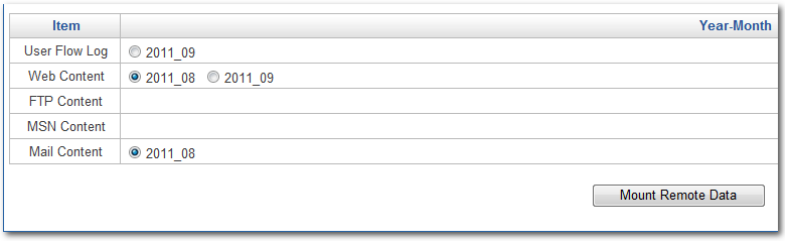

Backup Setting
Scheduled Backup
01:00
Send Backup Result Notification
Last Backup Time
2011-08-25 10:16:20 > Spend Time : 1 seconds, Remote Available Space : 47748 MBytes
Backup Now

Backup Item
There are five items: User Flow Log, Web Content, FTP Content, MSN Content, and Mail Content.

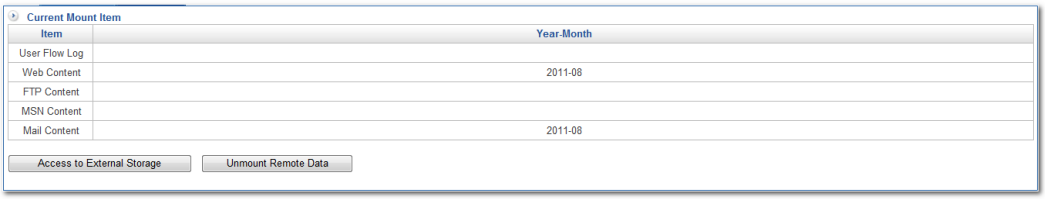
3.6.2 Data Mount

If you want to see previous contents, but you have ever reset machine to default setting or have ever Clear Data, for these reasons, there are no data contents in this machine hard disk. Fortunately, you have ever use Backup & Mount application to backup contents to another server or computer. Then, you can mount these contents to search for Content Record items.

First please click on Access to External Storage
You will see data items that you have ever backup.



Click on Mount Remote Data

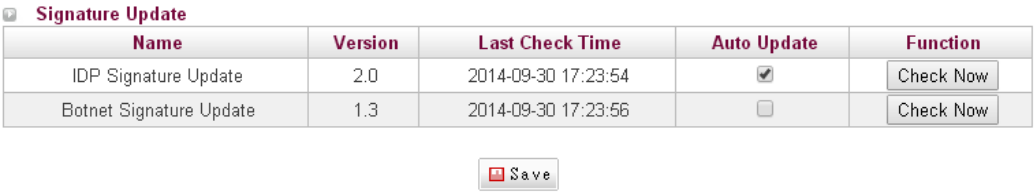


Click on Unmount Remote Data
Click on Unmount Remote Data if user does not want to search for Remote Data contents.

3.7 Signature Update

IFW320 provides auto signature update. In this section, it describes configuration samples of IDP and BotNet signature update. The updates consist of the latest released signatures, which allow them to prevent, detect and remove malware.

3.7.1 Signature Update



To select update items, check the box. User can check the update item, and enable "Auto Update."

Click on Check Now
Then signatures can be updated to the latest version.

3.8 CMS

CMS is Central Management System. This application not only allows you to view each one of the IFW320 equipment over the network and Internet, but also allows you to backup each configure setting or update firmware from head office. For example, you can have four IFW320 in one building or different places, and be able to view each IFW320 interfaces from all of them on the same screen or monitor.

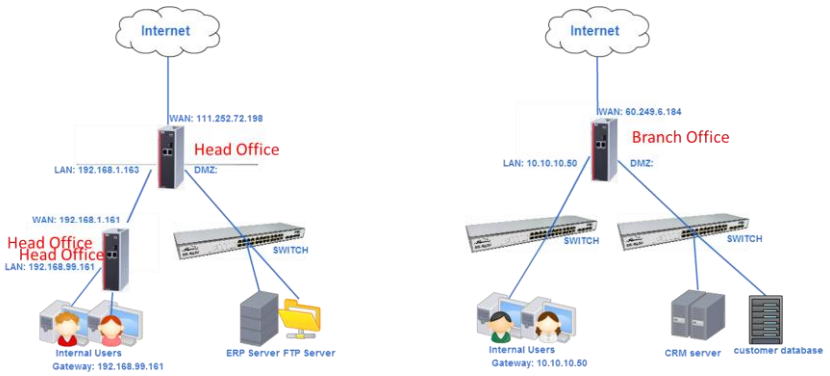
3.8.1 CMS Setting

Select *Configuration* > *CMS* > *CMS Setting*.

Example

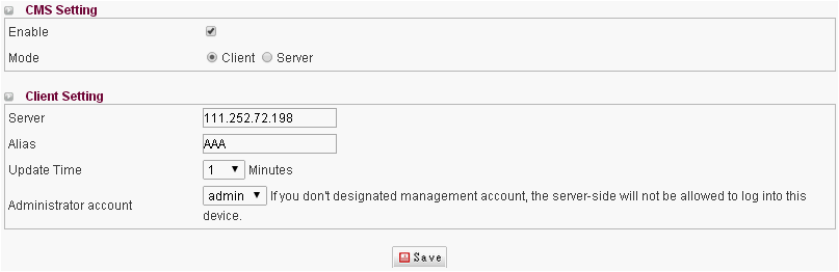
Assume:

Head office: WAN IP = 111.252.72.198 and LAN IP = 192.168.1.163.
Head office-A: office WAN IP = 192.168.1.161 and LAN IP = 192.168.99.161.
Branch office: WAN IP = 60.249.6.184 and LAN IP = 10.10.10.50.
And the CMS network architecture is given as follows:



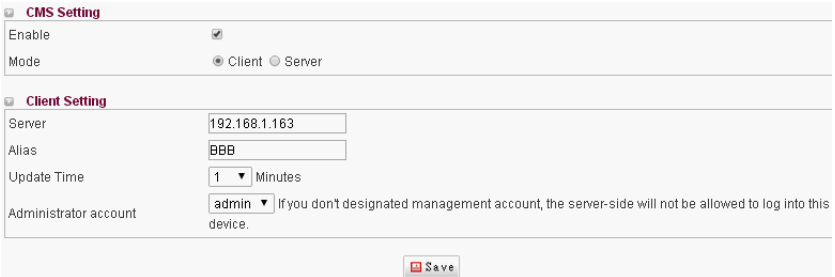
Client site

Branch office:



Mode: Client.
Server: Enter head office WAN IP 111.252.72.198 or domain.
Alias: Enter a name for recognition.
Click on Save ***.***

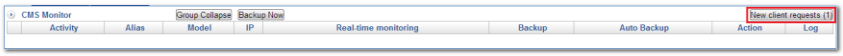
Head office-A office:



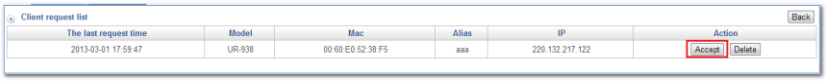
Mode: Client.
Server: Head office and head office-A are at the same internal subnet, so enter head office LAN IP 192.168.1.163 or domain.
Alias: Enter a name for recognition.
Click on Save ***.***

Server site

Head office:
Click "New client requests (1)".

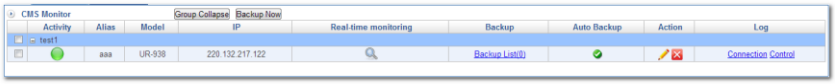


Click "Accept": You will see the following figure showing CMS client(s).



And you will see the following figure showing CMS client site information.

The following figure shows CMS Lists.

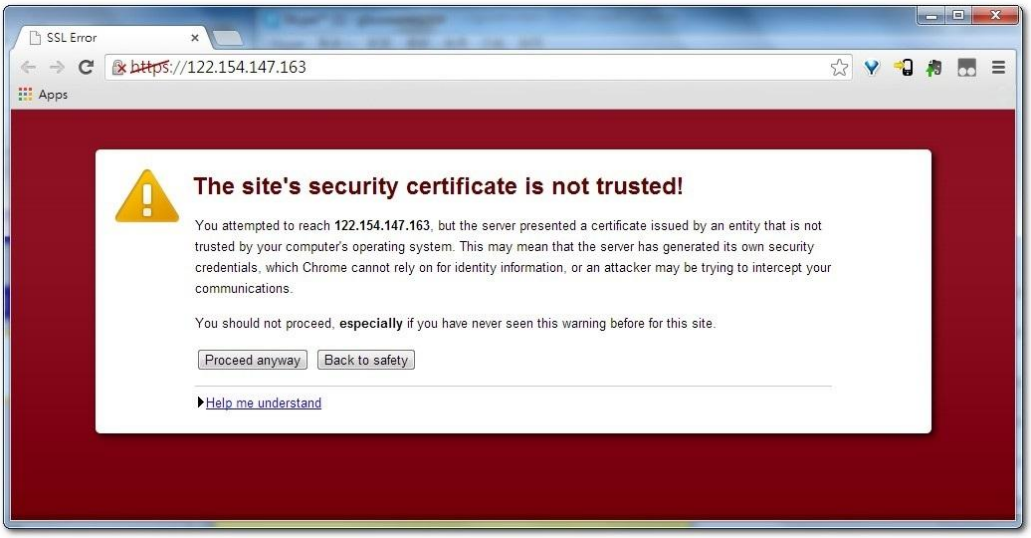


: Connect succeed.

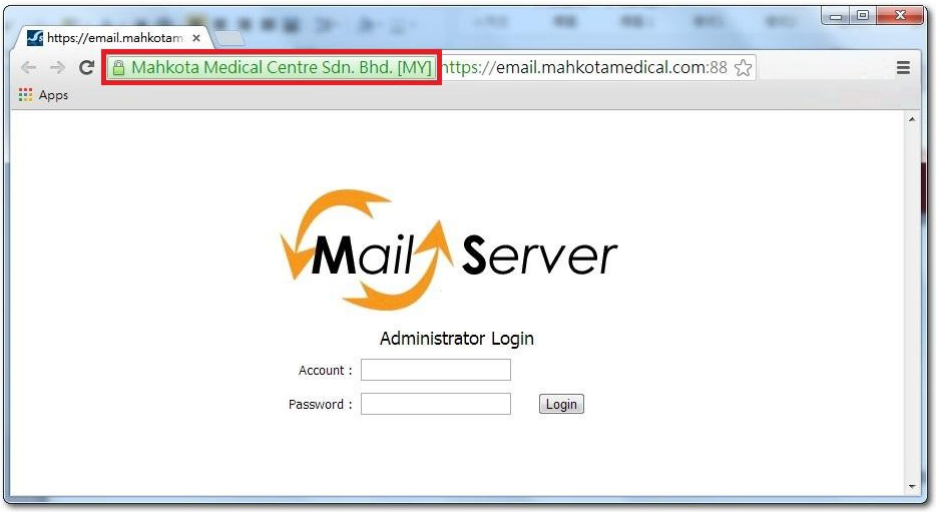
: Connection failed.

3.9 SSL Proof

If you don't like the general kind of SSL notification web page, please apply for your own SSL Certification at local SSL Certification organizations. It depends on company domain, your company WAN IP, company logo, and others. The following figure shows SSL Error screen.


SSL Error
https://122.154.147.163
Apps
The site's security certificate is not trusted!
You attempted to reach 122.154.147.163, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

It will show green browser if SSL Certification is installed, see figure below.



3.9.1 SSL Proof Set

Caution

Note that Axiomtek doesn't suggest and guarantee any one of SSL Certification organizations, the following are for examples only.

GeoTrust: https://www.geotrust.com

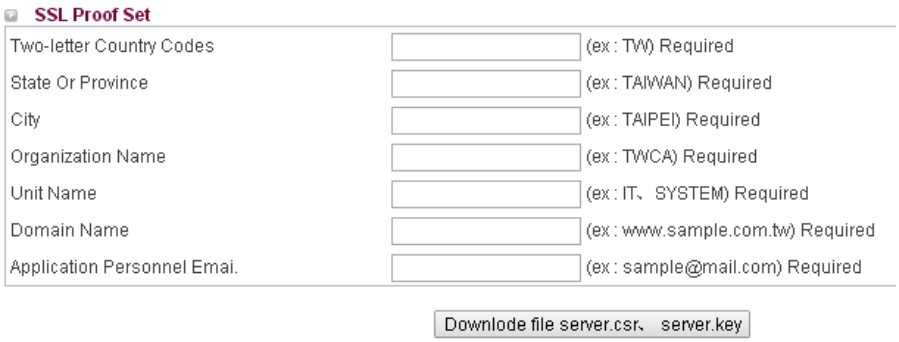
Symantec: http://www.symantec.com/verisign/ssl-certificates?inid=us_ps_flyout_prdts_ssl

StartSSL PKI: http://www.startssl.com/

Select *Configuration* > *SSL Proof*.

1. Please import three files (server.Key, server.crt, and intermediate certificate) which you apply for your own SSL Certification from SSL Certification organizations, see figure below.

2. Sometimes, organizations will ask for server.cst and server.key. Therefore, please enter information and download files. Offer these two files to SSL Certification organization.



Chapter 4
Network

In this chapter, Administrator can set the office network. There are two parts: Interfaces and Routing. The Administrator may configure the LAN and WAN IP addresses. Besides, it not only includes IPv4 address setting, but also IPv6 address settings.

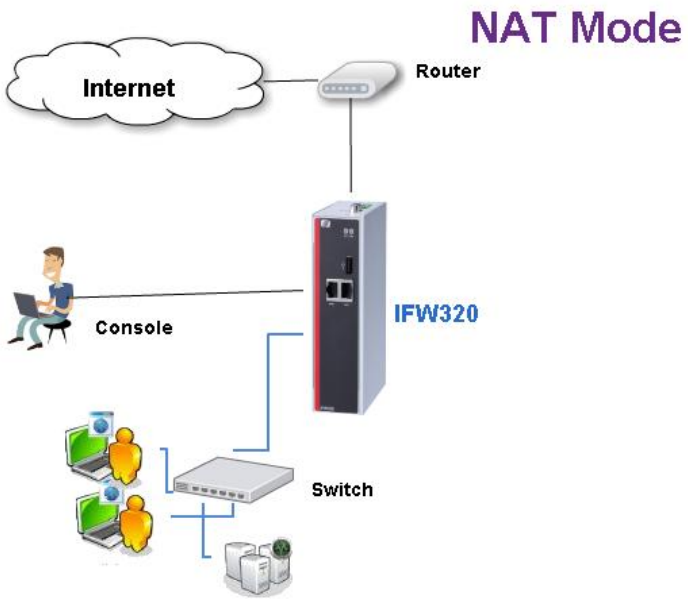
- Interfaces
- Interfaces (IPv6)
- Routing
- 802.1Q

4.1 Interface

IFW-320 is an industrial firewall to defend industrial networks by safeguarding sensitive control networks. Beginning with a pure firewall protection, it offers IDP, BotNet, WEB Filtering, VPN (IPSec, PPTP, SSL), authentication to secure remote security, etc. Network Administrators can set up different network entries, enable related security mechanism, and secure gateway based on their needs. This configuration process is also very similar on ordinary firewalls and IP switches.

Axiomtek IFW-320 can be configured in one of two primary methods, Bridge mode and NAT mode. Before running the base station, it is suggested to check your present network environment first. Please see the following configuration instructions:

1. **NAT Mode:**
   IFW-320 is suggested to be located behind a router and/or NAT device. Each port should be assigned to different segments, see figure below.



If NAT mode is adopted to be the operational mode, please refer to the following form for more information before configuration.

Administrator Password		
Internal	IP: Netmask:	____.____.____.____.____ ____.____.____.____.____
WAN1	IP: Netmask:	____.____.____.____.____ ____.____.____.____.____
Network Settings	Default Gateway:	____.____.____.____.____
	Primary DNS Server: Secondary DNS Server:	____.____.____.____.____ ____.____.____.____.____

Administrator Password
System administrator password.

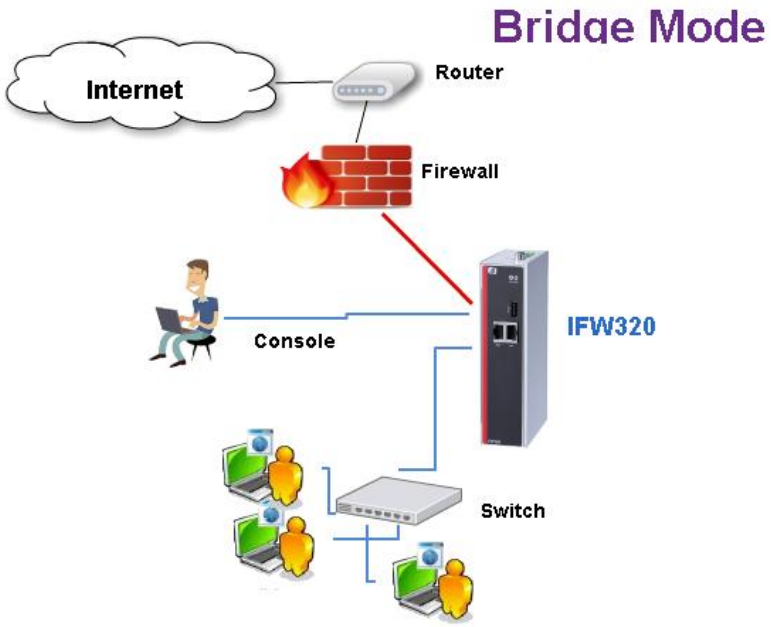
Internal Interface IP/Netmask
Use internal IP e.g. 192.168.1.99/255.255.255.0 (Always on the internal network segment).

External Interface IP/Netmask
Use external IP e.g. Line ISP and ADSL. Apply IP e.g. 39.120.84.132/255.255.255.0.

Default Gateway
Default route that connects to routers of the external interface port or IP addresses for an ADSL router.

DNS Server IP
Internal DNS server and external DNS server.

2. Bridge Mode:
IFW-320 is suggested to be located behind a router, firewall, and/or NAT device. In bridging, LAN IP can be set up and the mode should be changed from NAT to Bridge in the internal network. See figure below.



If Bridge mode is adopted to be the operational mode, please refer to the following form for more information before configuration.

Administrator Password		
Management IP	IP: Netmask: Default Gateway:	____.____.____.____.____ ____.____.____.____.____ ____.____.____.____.____
DNS Settings	Primary DNS Server: Secondary DNS Server:	____.____.____.____.____ ____.____.____.____.____

Administrator Password
System administrator password.

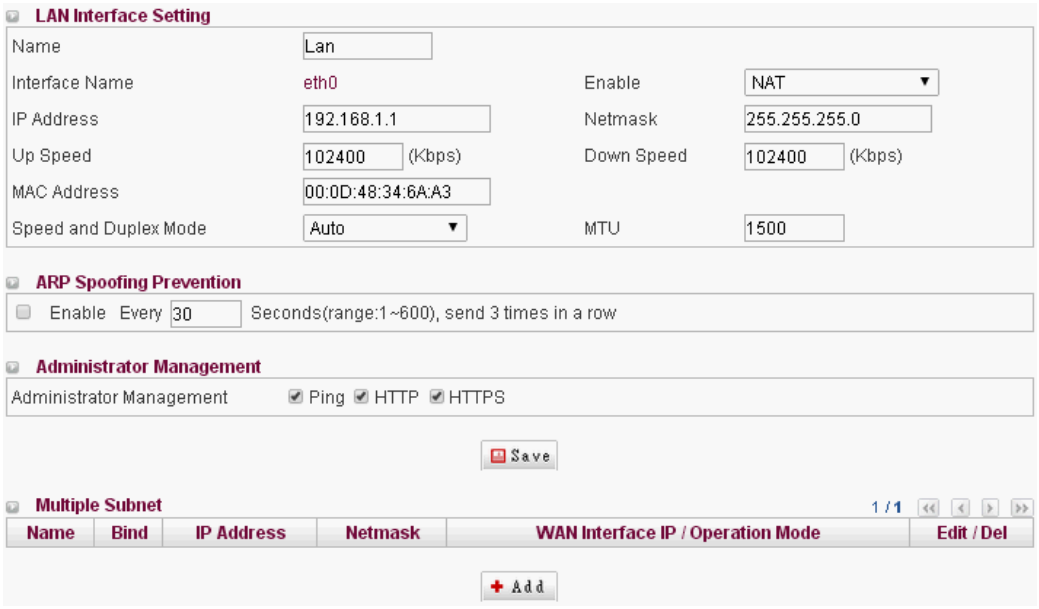
Management IP
Administrative Interface.

DNS Server IP
Internal and external DNS server.

In the Interface section you can enable the following lists:

4.1.1 LAN

Select *Network* > *Interface* > *LAN*. The LAN Interface Setup is as follows:



Name
Enter any word for recognition.

Interface Name
eth0.

IP Address
Enter an IP address.

Netmask
Enter a Netmask.

Up Speed
Define a suitable maximum Upstream bandwidth for each for them in order that the device may use it as a basis for operating.

Down Speed
Define a suitable maximum Downstream bandwidth for each for them in order that the device may use it as a basis for operating.

MAC Address
Enter a MAC Address.

Speed and Duplex Mode
Select which network speed is suitable for user.

Caution ***(10Mb/Half).***

MTU
Default setting is 1500.

Click on Save **.**

ARP Spoofing Prevention

Note ***With ARP spoofing (also known as ARP poisoning) you are tricking your target into thinking that you are the device who they want to send its data to. So for example you want all Internet traffic from the target to go to your machine, you would tell the target that your machine's MAC address is the MAC address of the gateway. Then you would want to tell the gateway that the target's MAC address is yours. In this way both side of the traffics flow to your machine. Start up your favorite packet sniffer and you are good to go. Of course you will want to make sure that you are forwarding the data and not storing it, if not your target won't be able to send data to its original destination.***

Multiple Subnet

Name
Enter any word for recognition.

Bind to Interface
Select it to start multiple subnet function.

IP Address
The multiple subnet range of IP addresses.

Netmask
Enter Netmask.

WAN Interface IP Address
The WAN IP addresses that the subnet corresponds to WAN.

Operation Mode
Allows the internal network to accommodate multiple subnets and enables Internet access through various external IP addresses. It displays using modes of WAN interface IP.
1. NAT
2. Routing

The completed multiple subnet is shown in figure below.

Example

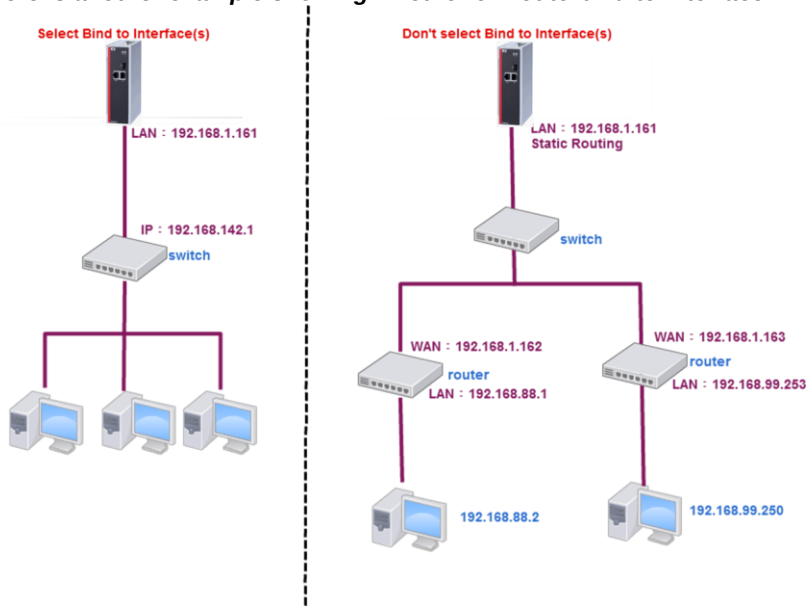
For example:
A company, divided into R&D department, customer service department, sales department, purchasing department and accounting department, has a lease line with multiple real IP addresses; 168.85.88.0/24. In order to facilitate the network management, the IT administrator may designate a subnet to each department respectively. The subnet distribution is as follows:
R&D Department:
192.168.1.1/24 (Internal) > 168.85.88.253 (External)
Customer Service Department:
192.168.2.1/24 (Internal) > 168.85.88.252 (External)
Sales Department:
192.168.3.1/24 (Internal) > 168.85.88.251 (External)
Purchasing Department:
192.168.4.1/24 (Internal) > 168.85.88.250 (External)
Accounting Department:
192.168.5.1/24 (Internal) > 168.85.88.249 (External).

Note

The IT administrator must renew his/her own PC's IP address upon using a DHCP server. It is to assure the access validity of the management interface after the change of LAN interface IP address. To renew the IP address distributed by a DHCP server, you may simply follow two steps:
1. ***Reboot computer.***
2. ***Enter "cmd" in the Run window, and enter "ipconfig /release", and then enter "ipconfig /renew", the IP address is successfully retrieved.***

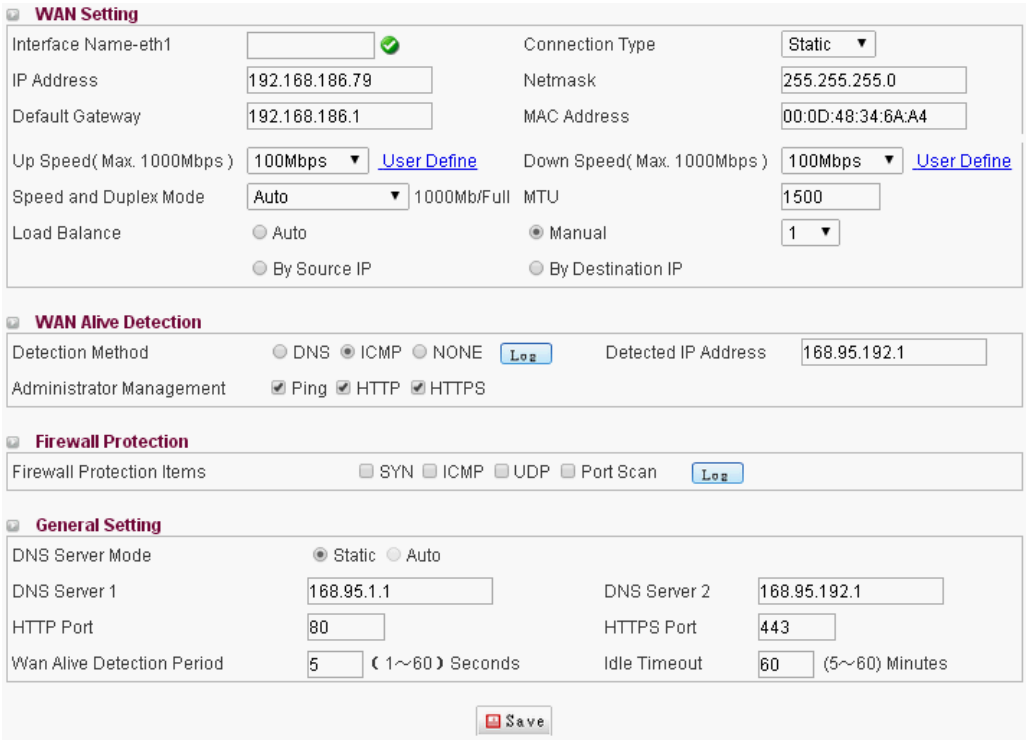
Example

Here is another example showing whether or not to bind to interface.



4.1.2 WAN

Select *Network* > *Interface* > *WAN*. The WAN Interface Setup is as follows:



Interface Name-eth1
Enter any word for recognition.

IP Address
Depend on the Connection Method. DHCP and PPPoE mode do not need to set IP address. Only Static mode needs to setup IP address.

Default Gateway
Depend on the Connection Method. DHCP and PPPoE mode do not need to set Default Gateway. Only Static mode needs to setup Default Gateway.

Up Speed (Max. 1000Mbps)
The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on Custom Define link to set your speed according to ISP's WAN Speed.

Speed and Duplex Mode
Usually, it sets on Auto. You also can select another setting.

Load Balancing
It offers four methods:
1. Auto: Distributes the outward sessions by the usage status of each WAN port.
2. By Source IP: For services that require using the same IP address throughout the process, such as online game and banking, IFW320 helps user retain the same WAN port (i.e. IP address) over which the session was created to avoid disconnection caused by the variation of the user's IP address.
3. Manual: According administrator demand to share loading on the WAN.
4. By Destination IP: Once a session is created between the IFW320 and a specific host, then the following sessions linking to that host will be automatically distributed to the same WAN port.

Connection Method
There are three Connection methods:
1. Static: Static IP address.
2. DHCP: Using DHCP to get IP address from ISP.
3. PPPoE: PPPoE.

Netmask
Enter a Netmask. Default setting is 255.255.255.0.

MAC address
Enter a MAC address.

Down Speed
The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on Custom Define link to set your speed according to ISP's WAN Speed.

Check Method
Using DNS, ICMP or NONE to check whether WAN is on or off. Both DNS and ICMP need to setup IP address for test.
1. DNS: Test the validity of Internet connection by requesting the domain name.
2. ICMP: Use ping command to test the validity of Internet connection.
3. NONE: Line is not detected; the connection status is always on line.

Management Service
There are three multiple-choice modes, ping, HTTP, and HTTPS. In addition, you can click on

to see more detail recorder.
1. Ping: The network can be detected by Ping commands when ticked.
2. HTTP: The management interface is available for accessing via HTTP protocol when ticked.
3. HTTPS: The management interface is available for accessing via HTTPS protocol when ticked.

Firewall Protect Items
There are four multiple-choice, SYN, ICMP, UDP, and Port Scan. It offers currently available protection. In addition, you can click on Log to see more detail recorder.

DNS Server 1
The IP address of the DNS server used for the bulk of DNS lookups. Default setting is 168.95.1.1

HTTP Port
HTTP port number for management. Default setting is 80.

WAN Check Time
System administrators can enter the system every interval of time to do more testing, unit calculated in seconds. Default setting is 3 seconds.

DNS Server 2
The IP address of the backup DNS server, used when the Primary DNS server is unreachable. Default setting is 168.95.192.1.

HTTPS Port
HTTPS port number for management. Default setting is 443.

Disconnect if idle for
The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection. The minute is a unit of time. Default setting is 60 minutes.

4.2 Interface (IPv6)

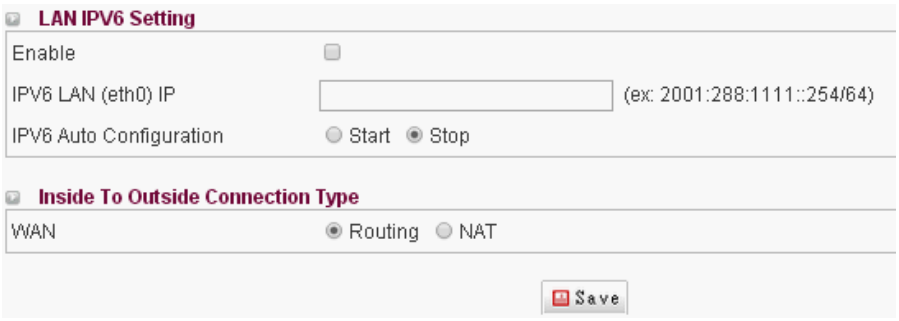
IPv4 is not enough anymore until 2021, and previously technical administrators are used to rely on IPv4 with NAT mode. As for now, IPv6 which offer more flexible for distributing IP address and routing table turn up. Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long and number about $4.3x10^{9}$ (4.3 billion). IPv6 addresses are 128 bits long and number about $3.4x10^{38}$ (340 Undecillion).

Note

IPv6 Auto Configuration is a new concept with IPv6. It gives an intermediate alternative between a purely manual configuration and stateful auto configuration.

4.2.1 LAN

Select *Network* > *Interface(IPv6)* > *LAN*.

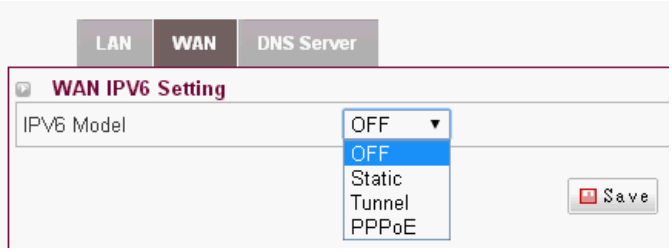


IPV6 LAN (eth0) IP
Enter IPv6 address.

IPv6 Auto Configuration
It's like IPv4 DHCP. It automatically distributes IPv6 address to among LAN internal users.

4.2.2 WAN

Select *Network > Interface(IPv6) > WAN*.



IPv6 Model
It offers 3 ways:
1. Static
2. Tunnel
3. PPPoE

4.2.3 DNS Server

Select *Network > Interface(IPv6) > DNS Server*.

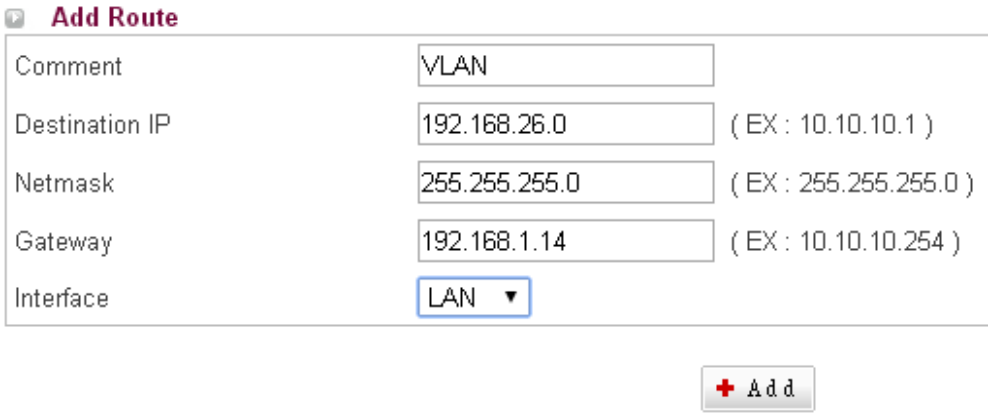
DNS IPv6 Setting
Please enter related DNS Server information.

4.3 Routing

The routing table lets the kernel know which block of IP addresses it can find behind which interface. Most of the lines which you see in the output contain information about your local networks. But since you need the firewall to have connections to the Internet, which in fact are all destinations with IP addresses which are not directly known to the kernel, an entry which sends all packets to a specific IP address in hope that host knows more about the delivery, is needed. That specific host is called default gateway. In the Routing section you can enable the following lists:

4.3.1 Routing Table

Select *Network* > *Routing* > *Routing Table*. Click on Add to create a new routing table.



Comment
Enter any word for recognition.

Destination IP
Enter an IP address.

Netmask
Enter a Netmask.

Gateway
Enter a Gateway.

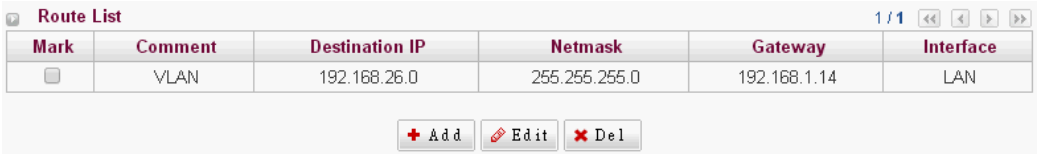
Example

For example:
A leased line connects Company A's Router 1 (10.10.10.1) with Company B's Router 2 (10.10.10.2).

Company A: Connect WAN port 1 (61.11.11.11) to ATUR; Connect WAN port 2 (211.22.22.22) to ATUR ; LAN subnet ranges 192.168.1.1/24 ; The LAN subnet that Router 1 (10.10.10.1, RIPv2 supported) connected to ranges from 192.168.10.1/24.

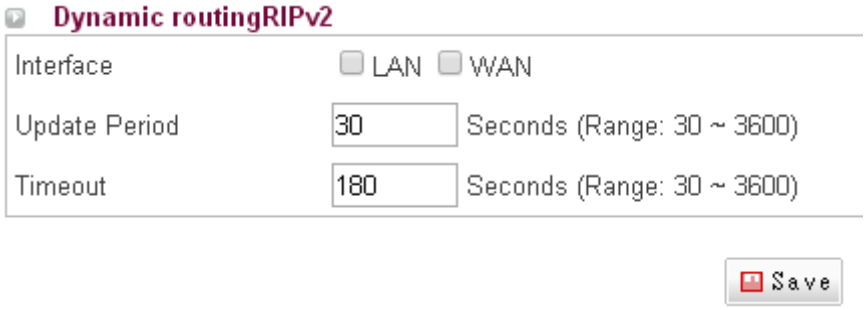
Company B: The LAN subnet that Router 2 (10.10.10.2, RIPv2 supported) connected to ranges from 192.168.20.1/24

Setting Routing Table completed, the network subnets of 192.168.20.1/24 and 192.168.1.1/24 now not only communicate with each other, but as well use NAT mode to access the Internet. In addition, select Mark tick box, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. Figure below shows the Routing Table list.



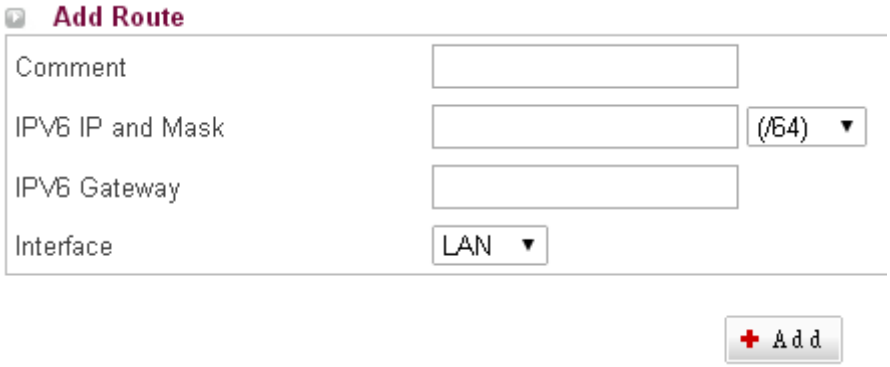
4.3.2 Dynamic Routing

Select *Network* > *Routing* > *Routing Table*. Click on Save to save Dynamic Routing. Check to choose LAN or WAN.



4.3.3 IPv6 Routing Table

Select *Network* > *Routing* > *Routing Table*. Click on Add to add IPv6 Routing Table. The IPV6 Routing Table is set in the same way as Routing Table section.



4.4 802.1Q

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The IEEE's 802.1Q standard was developed to address the problem of how to break large networks into smaller parts so broadcast and multicast traffic wouldn't grab more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks. In this section you can enable the following lists:

4.4.1 802.1Q

Select *Network* > *802.1Q* > *802.1Q*. Click on

to add VLAN ID.

Comment
Enter any word for recognition

IP Address
Enter an IP address.

The IP address = 10.10.10.1.

Example

Netmask
Enter a Netmask.

The Netmask = 255.255.255.0.

Example

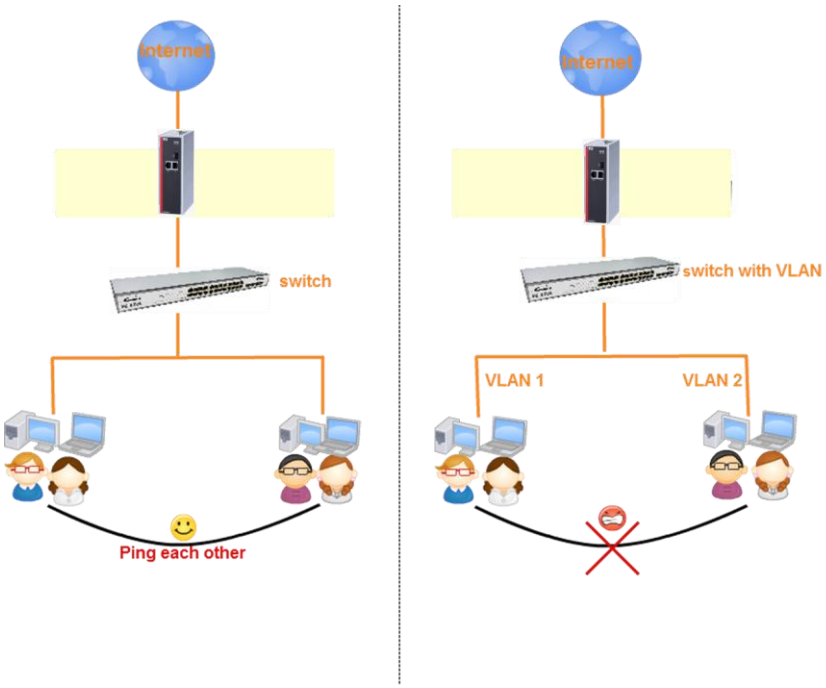
Interface
Select interface; LAN or WAN.

VLAN ID

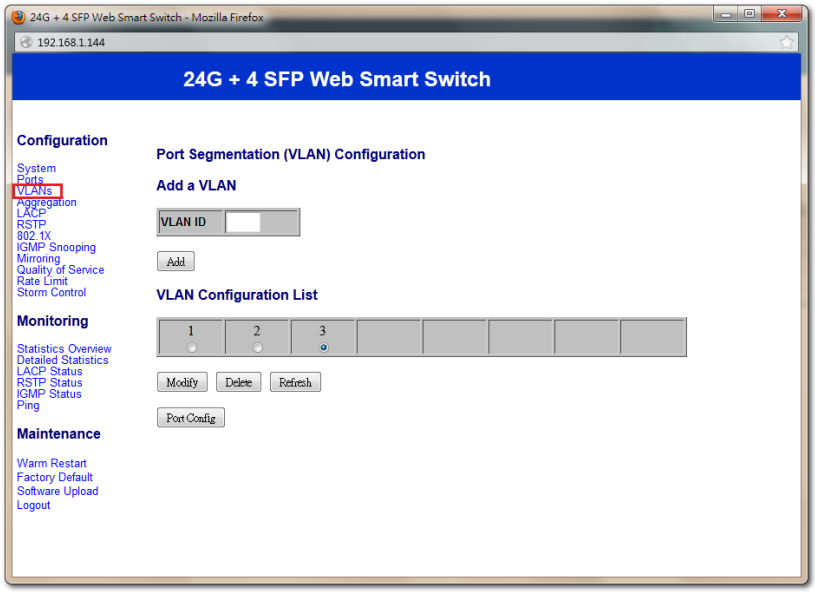
It is the identification of the VLAN, which is basically used by the standard 802.1Q.

Example

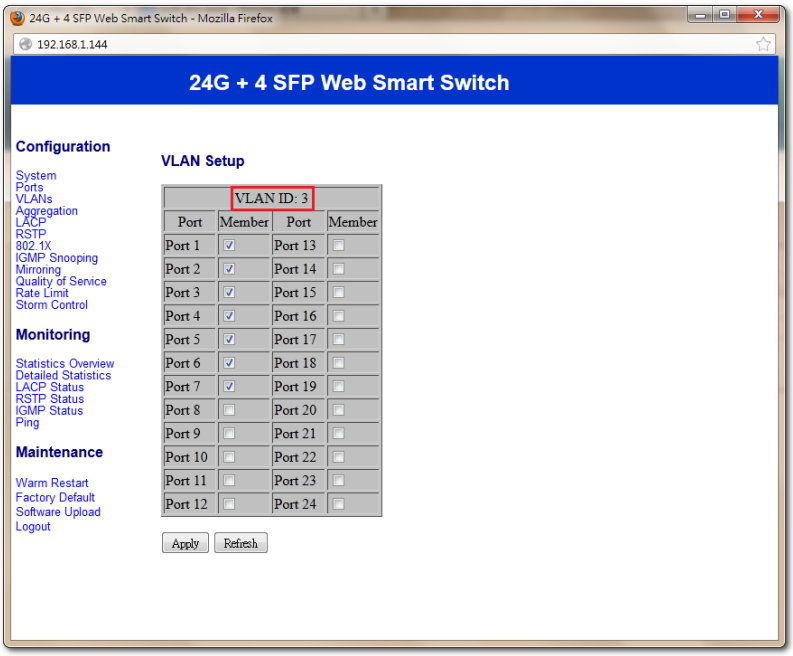
Here ML-9324 switch is taken as an example. The following figure shows differences between connection with or without VLAN.



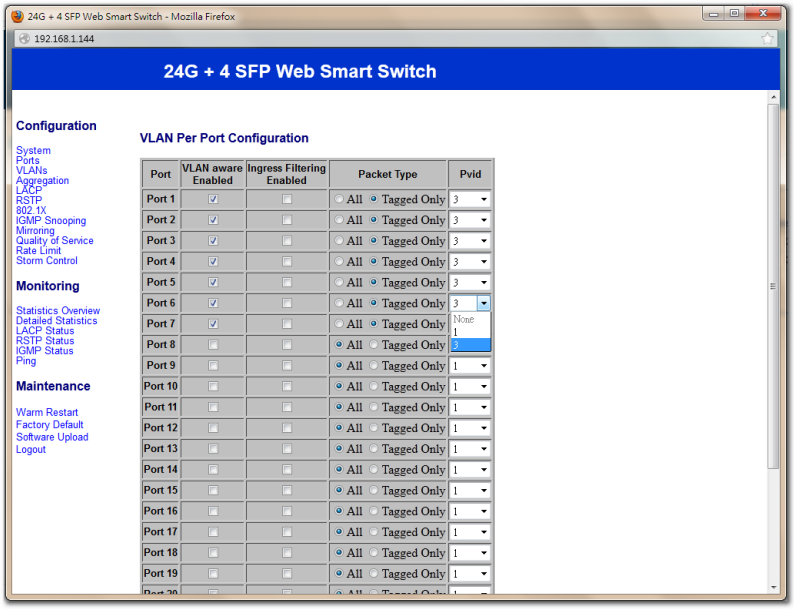
Check your switch setting. Let's create some VLANs.



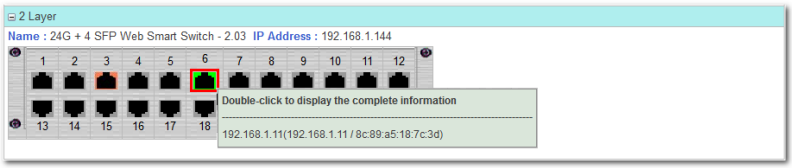
Then, distribute some ports among one group. Figure below shows the VLAN Setup.



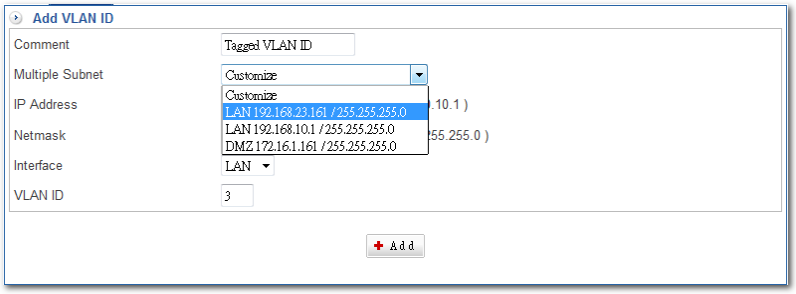
Select Port 1~Port 7 where packets should select Tagged 3.



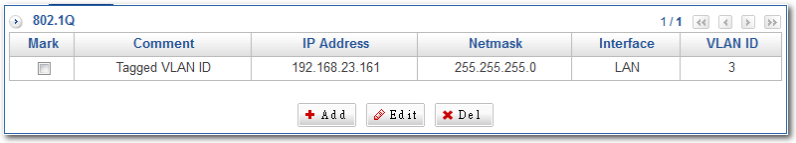
Your port is described in the following figure.



Add "VLAN ID 3" now, or otherwise port 6 cannot surf Internet.



The 802.1Q setting is finished, see figure below.



This page is intentionally left blank.

Chapter 5
Policy

IFW320 inspects each packet passing through the device to see if it meets the criteria of any policy. Every packet is processed according to the designated policy; consequently any packets that do not meet the criteria will not be permitted to pass. The items of a policy include Policy Name, Source Address, Destination Address, Action, Protocol, Service Port or Group, Software Access Control, QoS, Schedule, URL Policy, Internet Auth, Using Which WAN, Maximum Concurrent Sessions per IP Address, Drop Skype, WEB/FTP Anti-virus, IDP, Packet tracing, Traffic Analysis, WEB Recorder, IM Recorder, FTP Recorder, MSN Recorder, and Outgoing Mail. The IT administrator could determine the outgoing and incoming service or application of which data packets should be blocked or processed by configuring these items. On the other hand, IDP belongs to AW models.

- LAN Policy
- WAN Policy

5.1 LAN Policy and WAN Policy

In this section you can enable the following lists:

Policy Name
Enter any word for the description of the policy.

Source Address
Source address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.

Destination Address
Destination address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.

Action
It offers two kinds: Permit and Drop. When it is “Permit”, the policy will be passed. On the other hand, when it is “Drop”, the policy will be stopped.
1. Drop: Deny the Policy.
2. Permit: Allow the Policy.

Protocol
1. ALL
2. TCP
3. UDP
4. ICMP (ICMP = Internet Control Message Protocol)

Service Port or Group
The services are regulated. Available options are the system default services and the services that are customized in section 6.2 Services.

Software Access Control
It can restrict the use of application software. Set this function in Software Blocking in section 6.5 Application Control.

QoS
The guaranteed and maximum bandwidth settings. The bandwidth is distributed to users. Set this function in section 6.4 QoS.

Schedule
Activate as per the configured scheduled time. Set this function in section 6.3 Schedule.

URL Policy
It can restrict the access to any URL websites specified. Set this function in section 6.6 URL Filter.

Internet Auth
This requires users to be authenticated to create a connection. Set this function in section 6.9 Authentication.

Using Which WAN
It determines over which WAN interface's packets are permitted to pass through.
1. All: Packets are granted to pass through all interfaces once approved by the configured policy.
2. WAN: Policy approved packets may access WAN.

Maximum Concurrent Sessions per IP Address
It determines the maximum number of concurrent sessions of each IP address. If the amount of sessions exceeds the set value, new sessions will not be created.

Drop Skype
It can restrict the use of Skype protocol.

WEB/FTP Anti-virus
It filters viruses contained within files transferred over WEB, FTP protocol.

IDP
It can identify intrusion packets and react to them in a timely manner.

Pause
Temporarily disable the policy.

Start
Start the Policy.

Delete
Delete the Policy.

Edit
Edit the Policy.

Traffic Analysis

Click on this button, you can see the detail illustration of traffic analysis.

Packet tracing

Record Logs of packet transmissions managed by the policy. You can click on button to see packet logs.

This page is intentionally left blank.

Chapter 6
Objects

In this chapter you can enable the following lists:

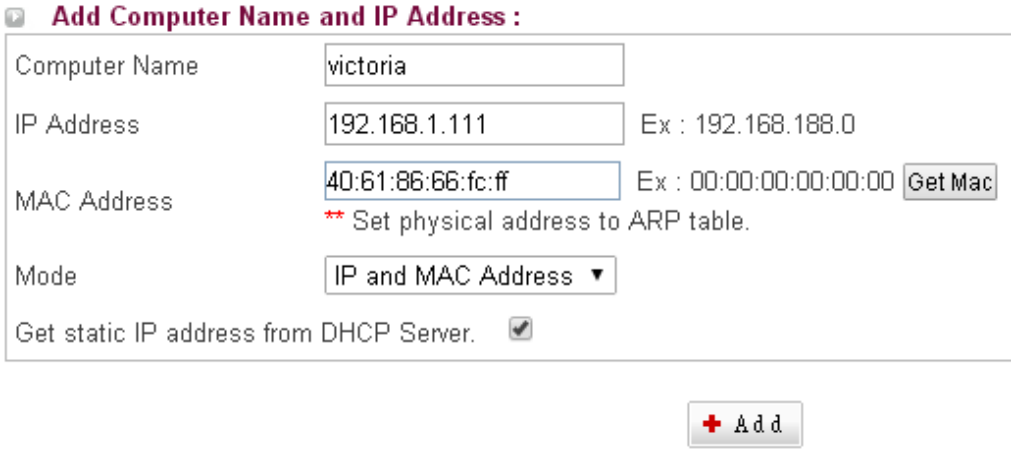
- Address Table
- Services
- Schedule
- QoS
- Application Control
- URL Filter
- Virtual Server
- Firewall Protection
- Authentication
- Bulletin Board

6.1 Address Table

In Address section, the IT administrator may configure network settings of LAN and WAN, as well as designate specific addresses in a network as a group. An IP address might represent a host or a domain, in either case, the IT administrator may give it an easily identifiable name for better management. According to the network in which an IP address resides, it can be categorized into two kinds, LAN IP address and WAN IP address. Each one can be organized into an address group comprising several addresses. Simply by applying the address group to a policy, the IT administrator may easily manage a group of users with merely one policy. In this section you can enable the following lists:

6.1.1 LAN IP Address

Select Objects > *Address Table* > *LAN IP Address*.



Select IP Mode
It offers two modes:
1. IPv4 Mode
2. IPv6 Mode

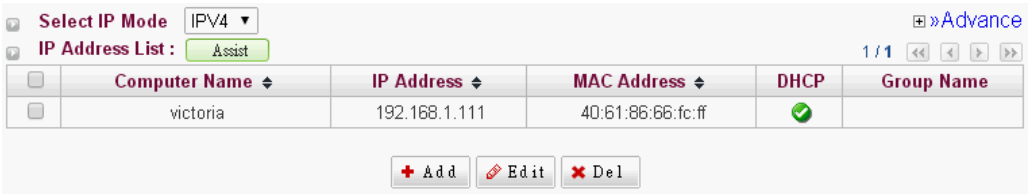
Computer Name, IP, and MAC Address
It is recommended to configure some desirable address names within Address first so that they are ready to use for the Source Address or Destination Address setting of a policy. In addition, you may click on Assist to add or create an entry.

Click on + Add
Create one LAN IP address first.

Mode Settings
1. Only set the IP address
2. Set IP and MAC address

Get static IP address from DHCP Server
Select static or dynamic IP address.

Setting LAN IP Address completed. In addition, select checkbox, and click on + Add to create a new sub-content, Edit to modify contents, or Del to cancel list.

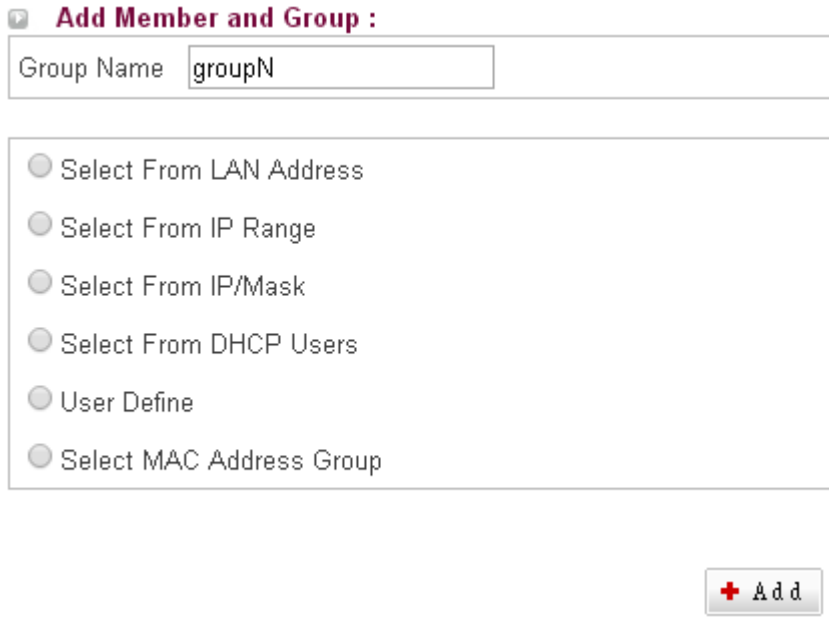


6.1.2 LAN Group

Select Objects > *Address Table* > *LAN Group*.

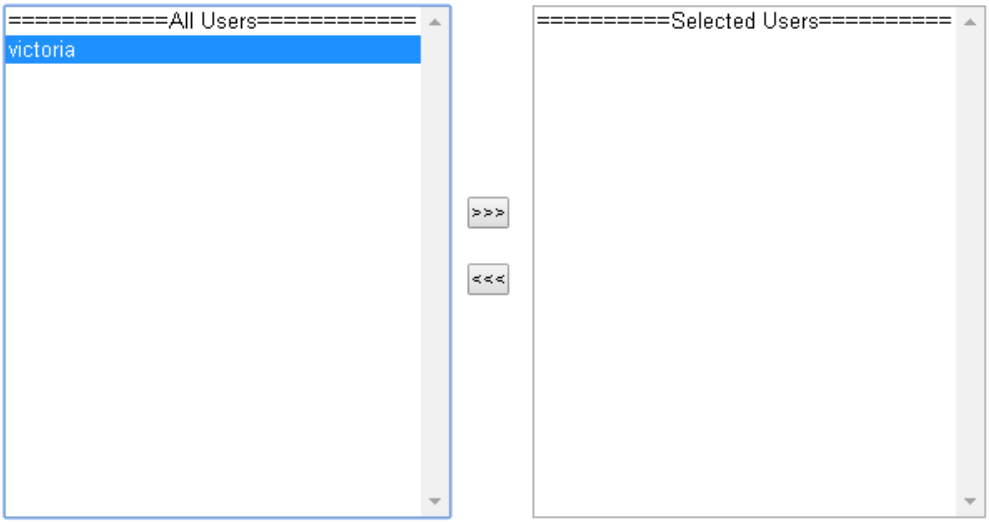
Select IP Mode
It offers two modes:
1. IPv4 Mode: IPv4 Address
2. IPv6 Mode: IPv6 Address

Click on + Add
Create a LAN Group rule.



Group Name
Enter any word for recognition.

Select From LAN Address
The left user lists which you add in LAN IP Address.



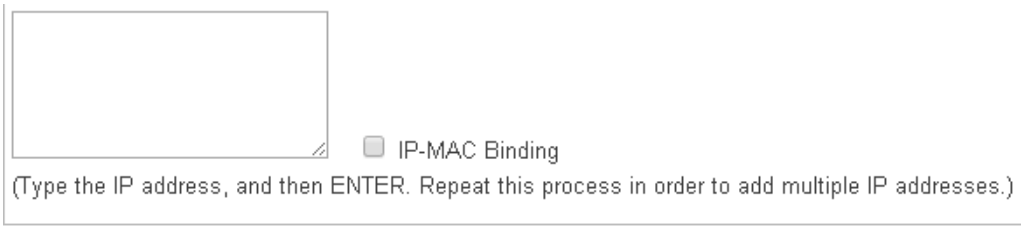
Select From IP Range
Enter the range of IP addresses which you want to restrict to.

Select From IP/Mask

Select From DHCP Users
It shows range of DHCP users, and these will be restricted. If you select “IP-MAC Binding” tick box, it will show list of IP MAC.

Select Users Define

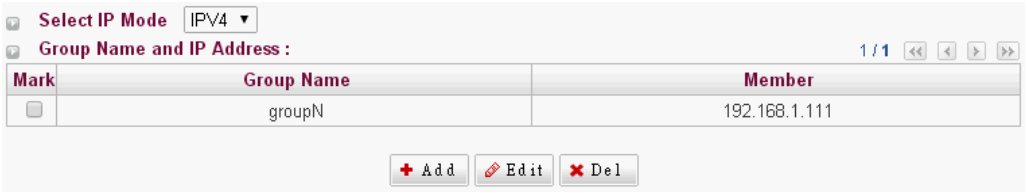
Please enter an IP address or subnet.



Select MAC Address Group

Please enter an MAC address or subnet.

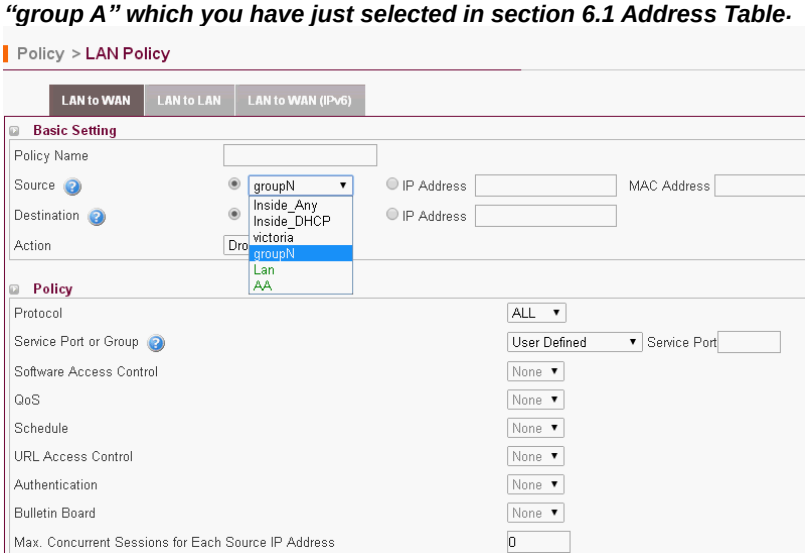
Setting LAN Group completed. In addition, select Mark tick box, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



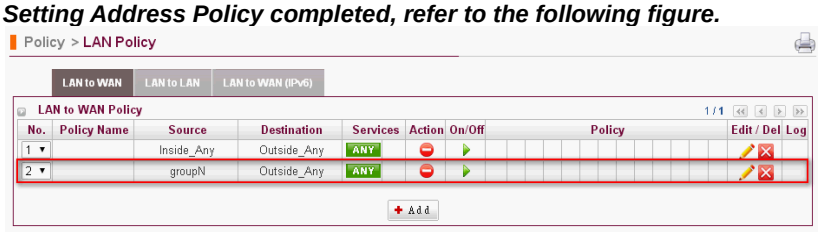
Example

Here is an example showing how LAN Group is used.

1. ***Select Policy > LAN Policy > LAN to WAN.***
2. ***Click on*** Add ***, and set Action to "Drop", and then set Source to "group A" which you have just selected in section 6.1 Address Table.***

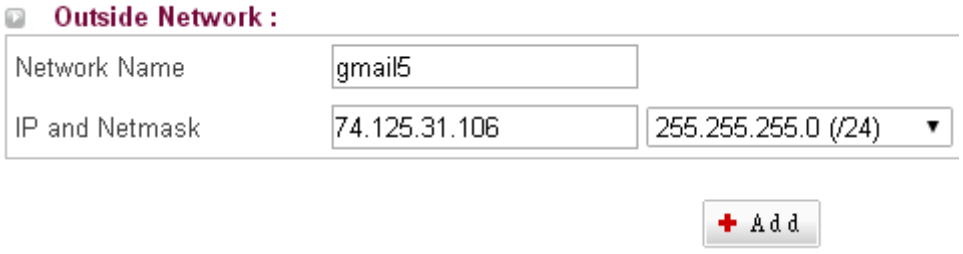


3. ***Setting Address Policy completed, refer to the following figure.***

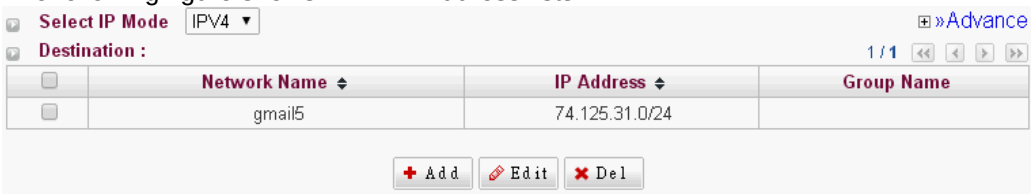


6.1.3 WAN IP Address

Select Objects > *Address Table* > *WAN IP Address*. The WAN IP Address is set in the same way as LAN IP Address.

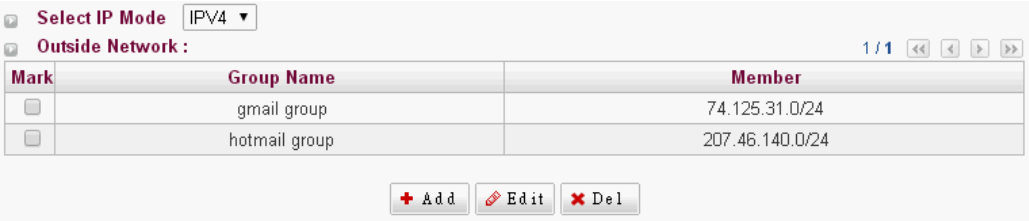


The following figure shows WAN IP Address lists.



6.1.4 WAN Group

WAN Group is set in the same way as LAN Group. When you want to use WAN Group, just select *Policy > WAN Policy> WAN to LAN*. Click on Add, and set Action to "Drop", and then set Source to which you have just set in section 6.1 Address Table. The following figure shows WAN Group lists.



6.2 Services

TCP and UDP protocols support a variety of services, and each service consists of a TCP port or UDP port number, such as TELNET (23), FTP (21), SMTP (25), POP3 (110), etc. This section has two types of services, that is, Pre-defined service and Service group. Pre-defined service includes the most common-used services using TCP or UDP protocol. It allows neither modification nor deletion while Custom service allows modification on port numbers based on the situation.

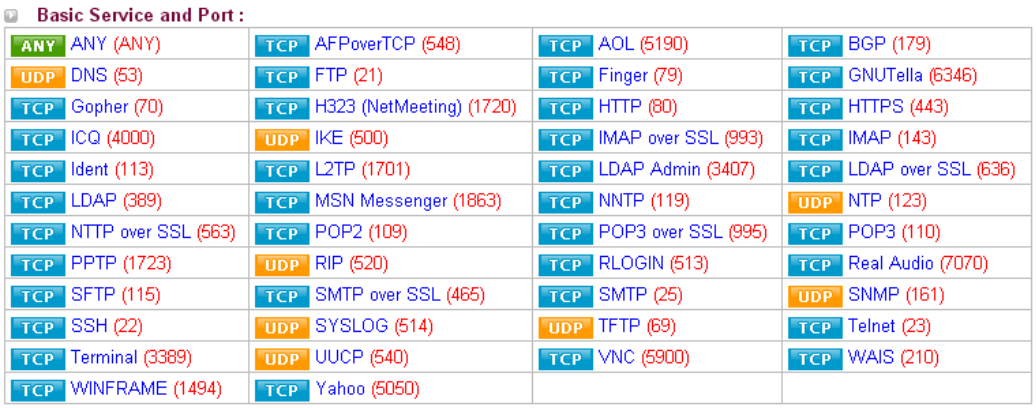
Caution

When configuring Custom service, the port number setting for either client port or server port falls between 0 and 65535. The IT administrator merely needs to determine the necessary protocol and port number for each Internet service, and then the client will be able to access different services.

In this section you can enable the following lists:

6.2.1 Basic Service

Select *Objects > Services > Basic Service.* The symbol and its description are shown in figure below.



Protocol
The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.

1. ANY: Any Service.
2. TCP: Services using TCP protocol, Gopher, ICQ, Ident, LDAP, NTTP over SSL, PPTP, SFTP, SSH, Terminal, WINFRAME, AFPoverTCP, FTP, H323 (NetMeeting), L2TP, MSN Messenger, POP2, SMTP over SSL, Yahoo, AOL, Finger, HTTP, IMAP over SSL, LDAP Admin, NNTP, POP3 over SSL, RLOGIN, SMTP, VNC, BGP, GNUTella, HTTPS, IMAP, LDAP over SSL, POP3, Real Audio, Telnet, and WAIS.
3. UDP: Services using UDP protocol, DNS, IKE, RIP, SYSLOG, UUCP, TFTP, NTP, and SNMP.

Port
Port number of the client user's PC which is used for connecting to the IFW320 device.

Caution

Range from 0 to 65535. Using default setting is recommended.

6.2.2 Service Group

To facilitate policy management, the IT administrator may create a service group including a group of necessary services.

Example

For example, ten users from ten different IP addresses request access to five types of services, namely HTTP, FTP, SMTP, POP3 and TELNET. It merely takes one policy with a service group to satisfy the service request of 50 combinations (10 users times 5 services equals to 50 service requests).

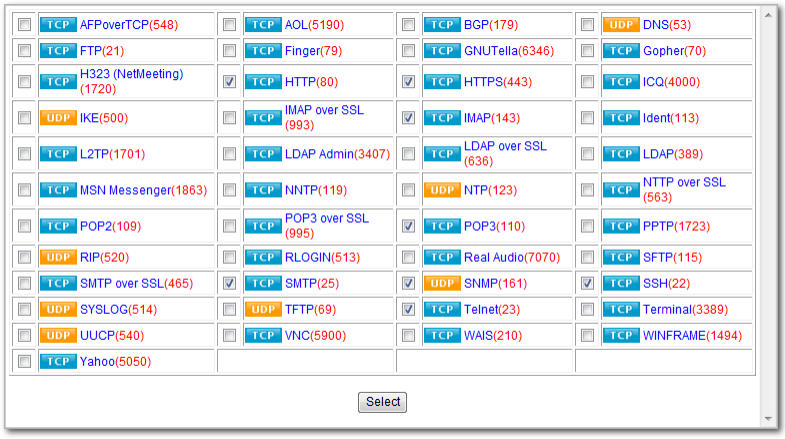
Select *Objects* > *Services* > *Service Group*. This function regulates the online usage of service.

Click on + Add
Create a Service rule.

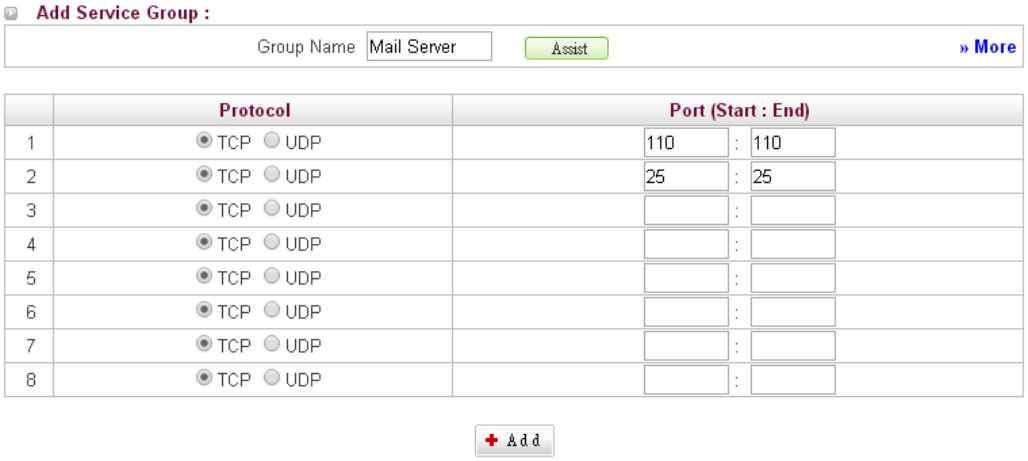
Service Name
Enter some words for recognition.

Click on Assist

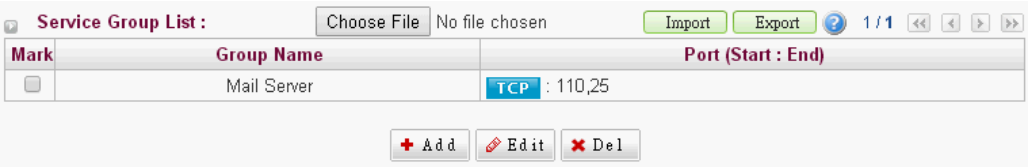
Select services. The figure below shows Service Assist View.



After services selection completed, if you made wrong selection and you want to remove one port, please clear the port.



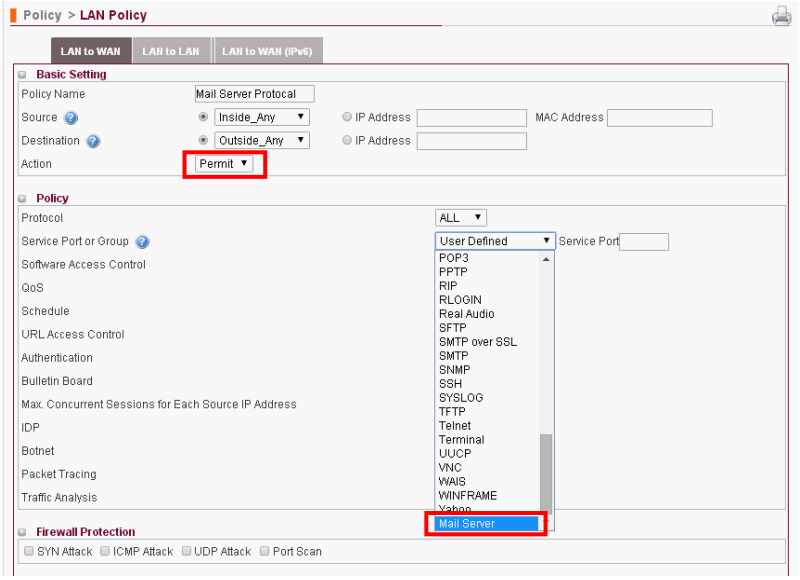
Setting Service Group completed. In addition, select ☑ checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



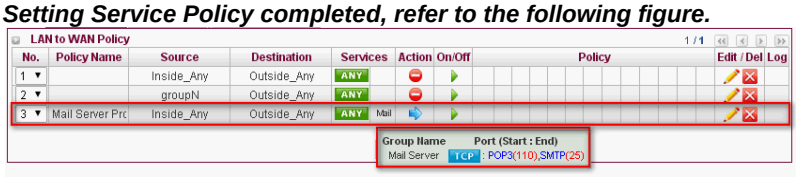
Example

Here is an example showing how Service Group is used.

1. ***Select Policy > LAN Policy or WAN Policy. Then select the function you need on the right side.***
2. ***Click on*** Add ***, and set Action to "Permit", and then set Service Port or Group to "Mail Server" which you have just selected in section 6.2 Services.***



3. ***Setting Service Policy completed, refer to the following figure.***

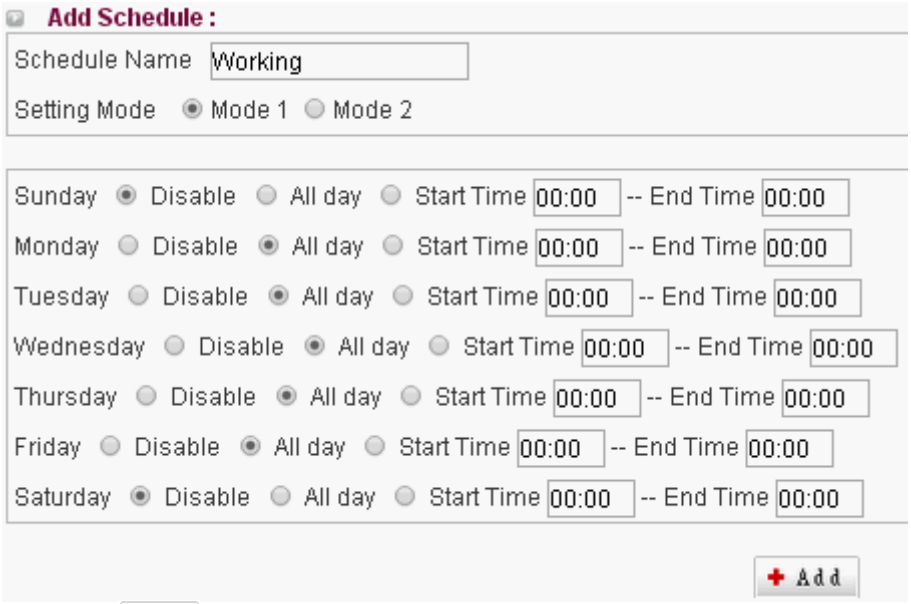


6.3 Schedule

The IT Administrator needs configure a schedule for policy to take effect and allow the policies to be used at those designated times. And then the Administrator can set the start time and stop time or VPN connection in Policy or in VPN. By using the Schedule function, the Administrator can save a lot of management time and make the network system most effective. In this section you can enable the following lists:

6.3.1 Schedule List

The system administrator and IT administrator can use Schedule to set up the device to carry out the connection of Policy or VPN during several different time divisions automatically. Select *Objects* > *Schedule* > *Schedule List*.


Add Schedule :
Schedule Name Working
Setting Mode Mode 1 Mode 2
Sunday Disable All day Start Time 00:00 -- End Time 00:00
Monday Disable All day Start Time 00:00 -- End Time 00:00
Tuesday Disable All day Start Time 00:00 -- End Time 00:00
Wednesday Disable All day Start Time 00:00 -- End Time 00:00
Thursday Disable All day Start Time 00:00 -- End Time 00:00
Friday Disable All day Start Time 00:00 -- End Time 00:00
Saturday Disable All day Start Time 00:00 -- End Time 00:00
Add

Click on Add

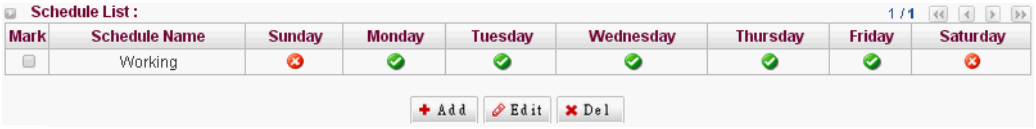
Click on Add to create a new Schedule rule first.

Schedule Name

Enter some words for recognition.

Then set your time schedule.

Setting Schedule List completed. In addition, select checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



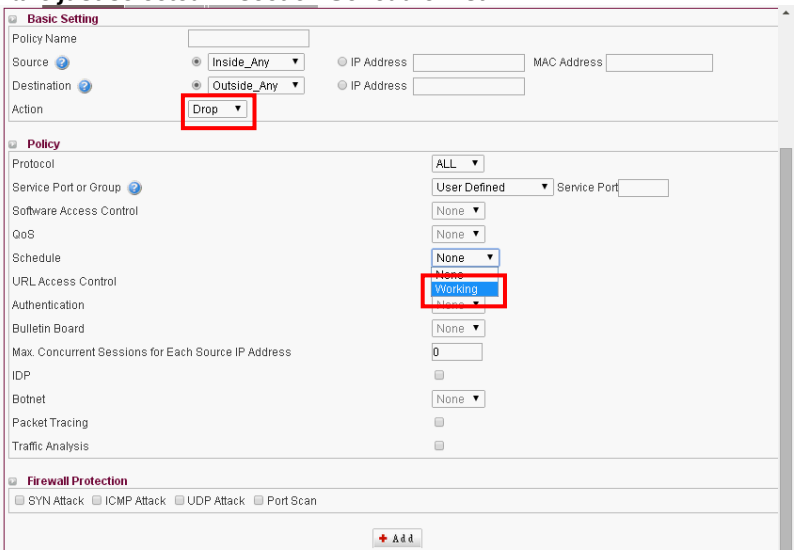
: Pass

: Disable

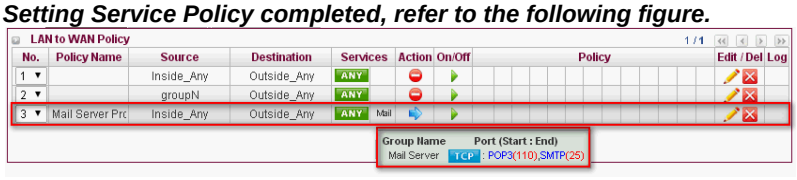
Example

Here is an example showing how Schedule List is used.

1. ***Select Policy > LAN Policy or WAN Policy. Then select the function you need on the right side. Here we use LAN to WAN for example. Click on*** Add ***first.***
2. ***Set Action to "Drop", and then set Schedule to "Working" which you have just selected in section Schedule List.***



3. ***Setting Service Policy completed, refer to the following figure.***



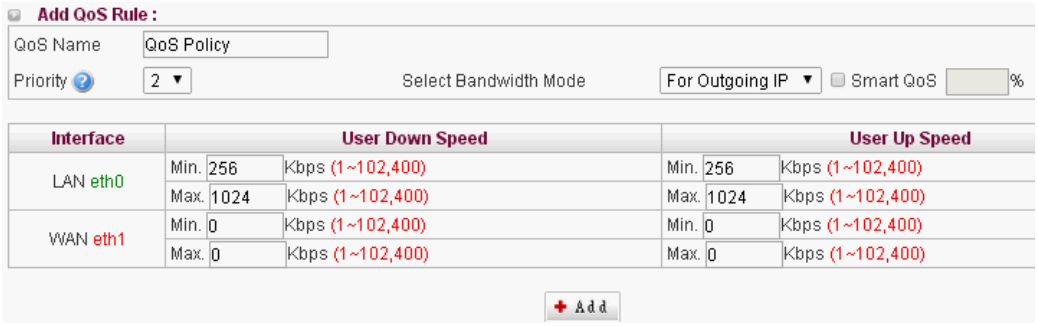
6.4 QoS

By configuring the QoS, IT administrator can control the Outbound and Inbound Upstream/Downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth. The QoS feature not only facilitates the bandwidth management but optimizes the bandwidth utilization as well. The following two figures indicate the improvement of bandwidth utilization as a result of enforcing QoS by showing before and after comparisons. In this section you can enable the following lists:

6.4.1 QoS Setting

Select *Objects* > *QoS* > *QoS Setting*.

Click on Add
Create a new QoS rule first



QoS Name
Enter any word for recognition.

Priority
Configure the priority of distributing Upstream/Downstream and unused bandwidth.

Bandwidth Mode
It offers three ways.

1. By Policy
2. Inside Per Source IP (It includes Smart QoS application)
3. Outside Per Source IP

Interface
Display LAN and WAN.

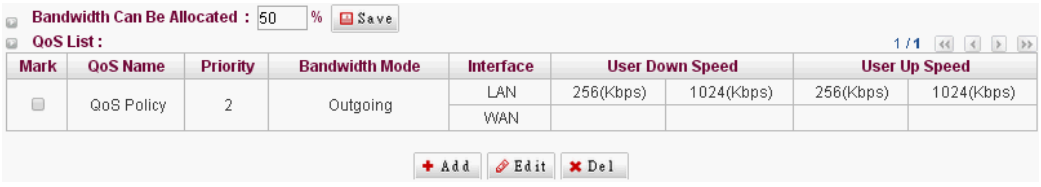
User Down Speed (Downstream Bandwidth)
Configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP.

User Up Speed (Upstream Bandwidth)
Configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP.

Min. (Guaranteed Bandwidth)
Specify the minimum (guaranteed) amount of bandwidth.

Max. (Maximum Bandwidth)
Specify the maximum amount of bandwidth.

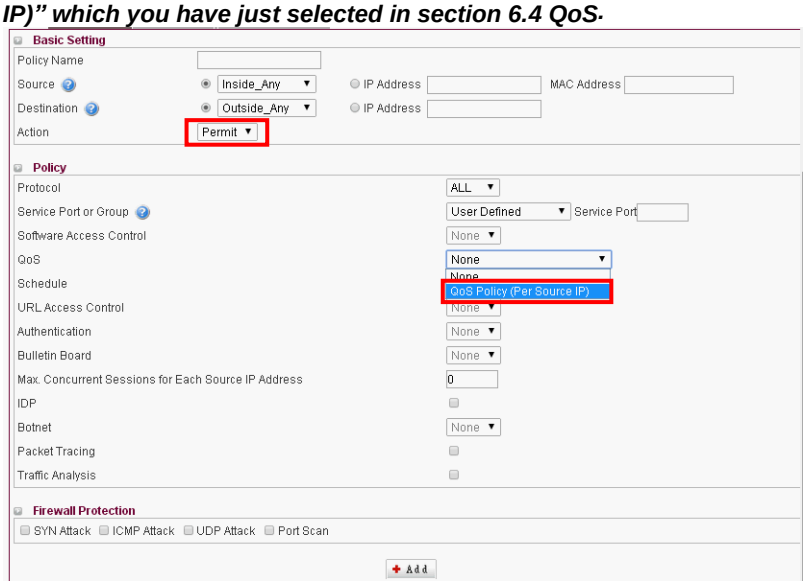
Setting QoS List completed. In addition, select checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



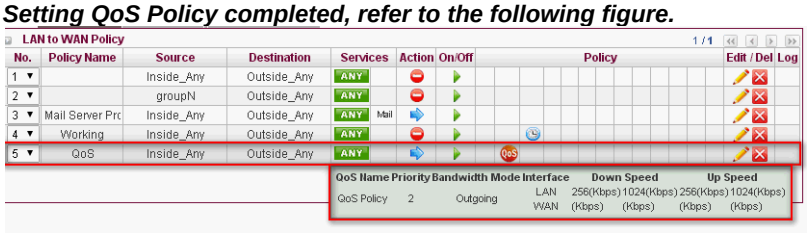
Example

Here is an example showing how QoS List is used.

1. ***Select Policy > LAN Policy or WAN Policy. Then select the function you need on the right side. Here we use LAN to WAN as example. Click on*** Add ***first.***
2. ***Set Action to "Permit", and then set QoS to "QoSPolicy (Per Source IP)" which you have just selected in section 6.4 QoS.***



3. ***Setting QoS Policy completed, refer to the following figure.***



6.5 Application Control

6.5.1 Setting

Select *Objects* > *Application Control* > *Setting*. It offers seven kinds of software blocking, File Sharing Application, Instant Messaging Client, VOIP Application Block, WEB application Block, WEB Mail Block, Game, Others. In this section you can enable the following lists:

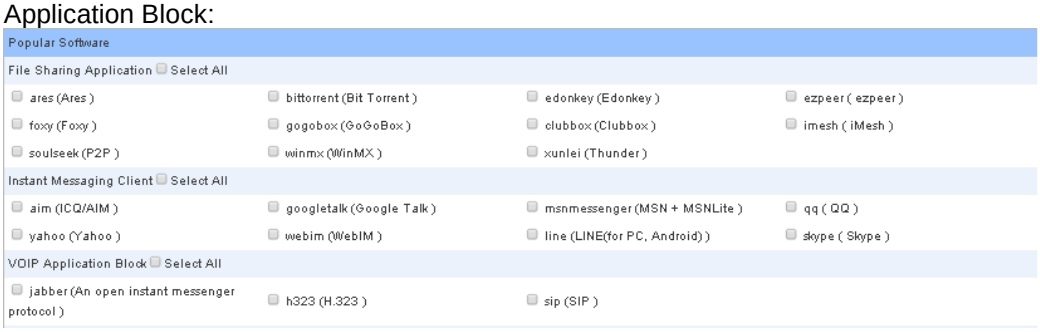
Click on Add

Click on Add first.

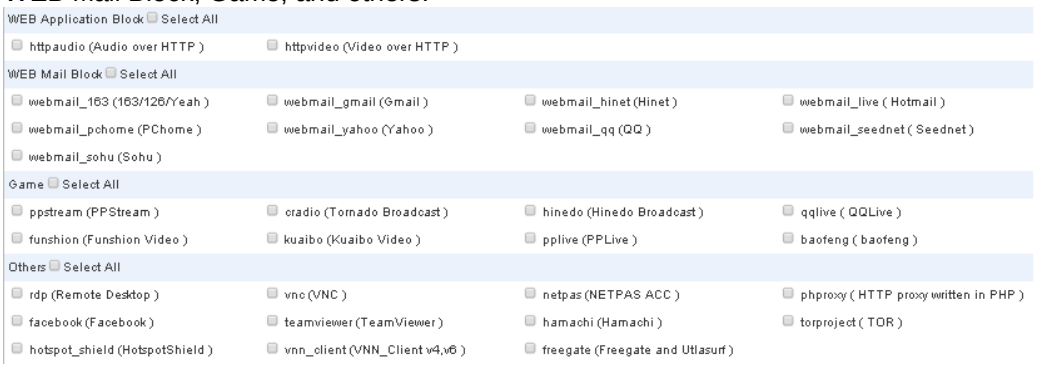
Group Name

Enter any word for recognition.

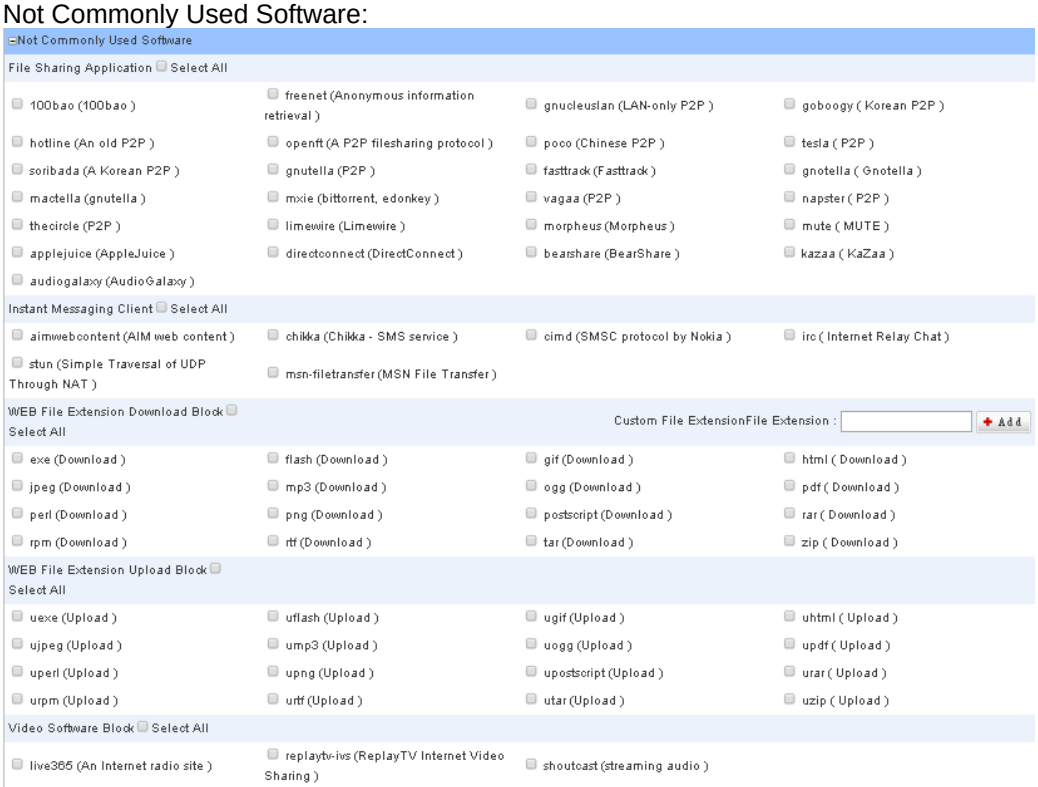
File Sharing Application, Instant Messaging Client, VOIP Application, and WEB Application Block:



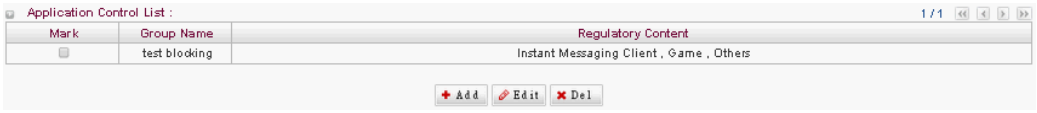
WEB Mail Block, Game, and others:



Not Commonly Used Software:



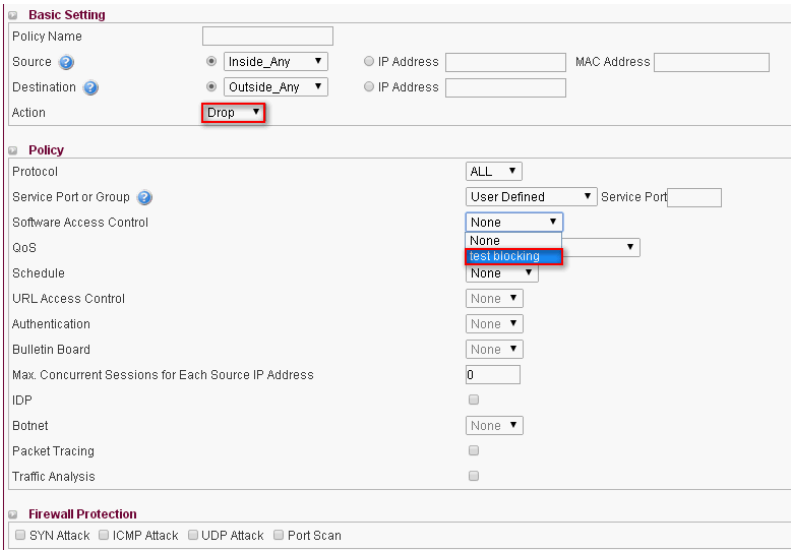
Setting Application Control List completed. In addition, select ☑ checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



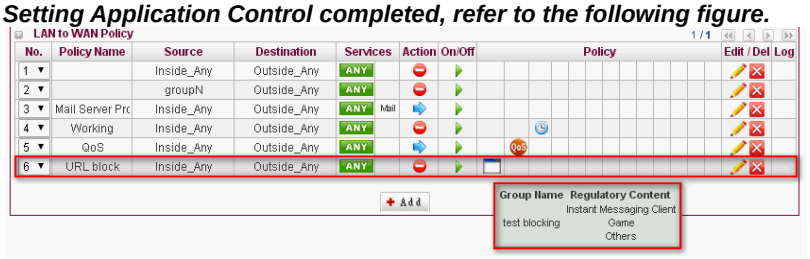
Example

Here is an example showing how Application Control List is used.

1. ***Select Policy > LAN Policy. Then select the function you need on the right side. Here we use LAN to WAN as example. Click on Add first.***
2. ***Set Action to "Drop", and then set Software Access Control to "test blocking" which you previously selected in section 6.5 Application Control.***



3. ***Setting Application Control completed, refer to the following figure.***

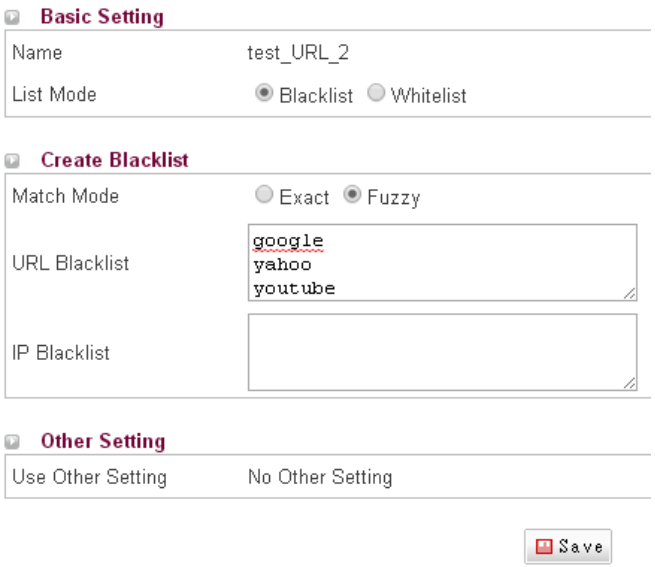


6.6 URL Filter

URL Filtering (URLF) is widely used for parental control, compliance and productivity. In schools, for instance, URLF is used to help deter exposure to inappropriate websites, such as pornography, nudity, aggressive sites, etc. In offices, URL filtering is especially an indispensable tool for web security policy. According to research, company employees spend a significant proportion of their time surfing non-work-related web during working hours. In addition to productivity, network latency is also an issue when employees surf unnecessary websites, or download bandwidth-intensive files. The greater concern is the threat caused from malicious applications or malware, while surfing some illegitimate or inappropriate websites. In this URL List section you can enable the following lists:

6.6.1 List Settings

Select *Objects* > *URL Filter* > *List Settings*. Click on Add.



Name
Enter any words for recognition.

List Mode
Select for Blacklist or Whitelist.

Match Mode
There are two ways, Exact and Fuzzy.

URL Blacklist
Enter the complete domain name or key word of the website. It is restricted specific website whether user surf Internet or not, however it depends on what you select on List Mode.

Example

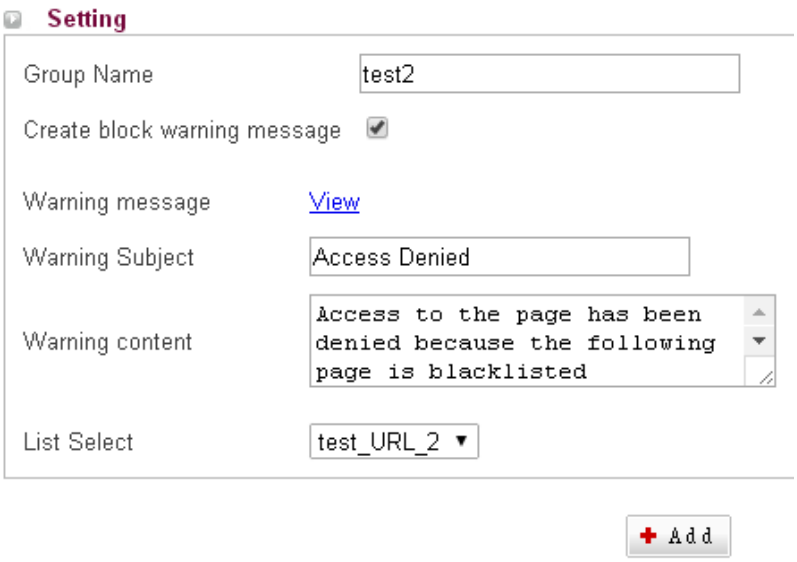
For example: "www.kcg.gov.tw" "kh.google.com" "gov" or "*google*".

IP Blacklist
Enter the complete IP address. It is restricted specific website whether user surf Internet or not, however it depends on what you select on List Mode.

Setting URL List completed. In addition, select Mark tick box, and click on Add to create a new sub-content, to modify contents, or to cancel list.

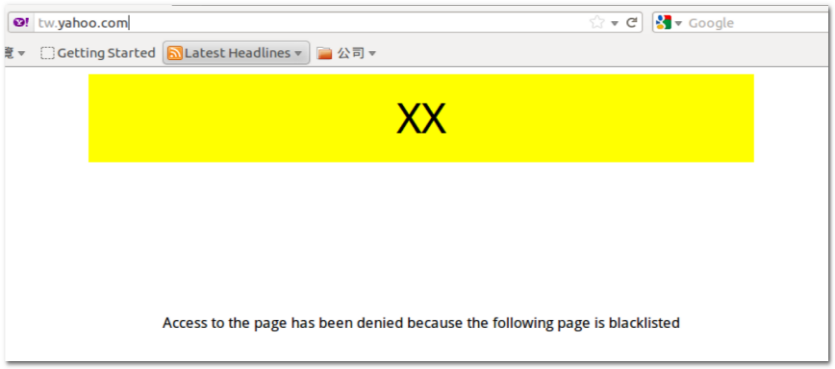
6.6.2 URL Settings

Select *Objects* > *URL Filter* > *URL Settings*. Then, click on Add.



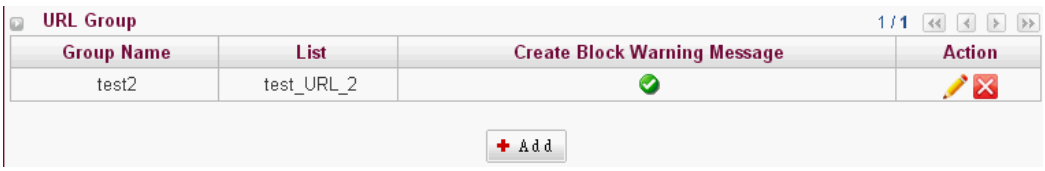
Group Name
Enter any words for recognition.

Create block warning message
Users can create their own block warning message if this checkbox is selected.



List Select
Pick an item that you previously added in List settings.

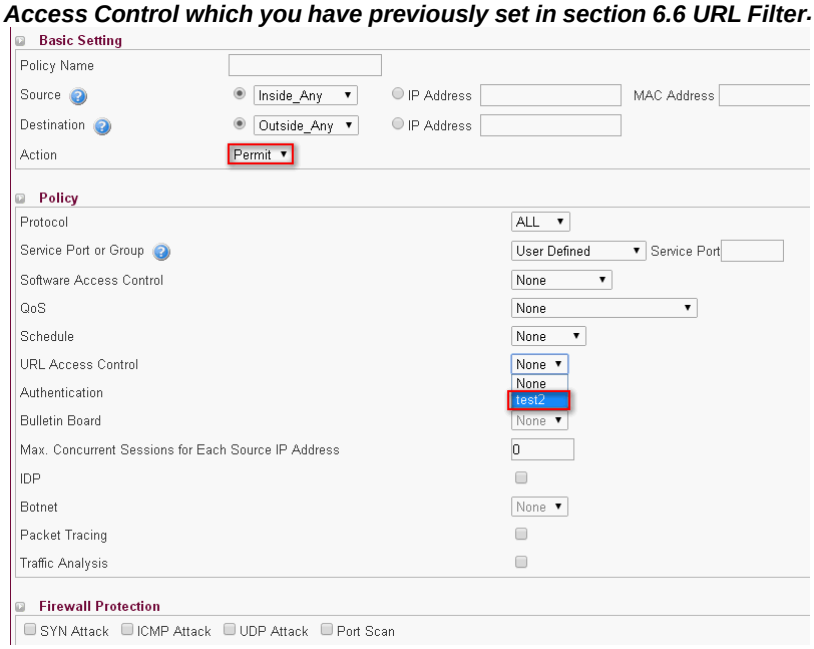
Setting URL completed. In addition, select Mark tick box, and click on Add to create a new sub-content, to modify contents, or to cancel list.



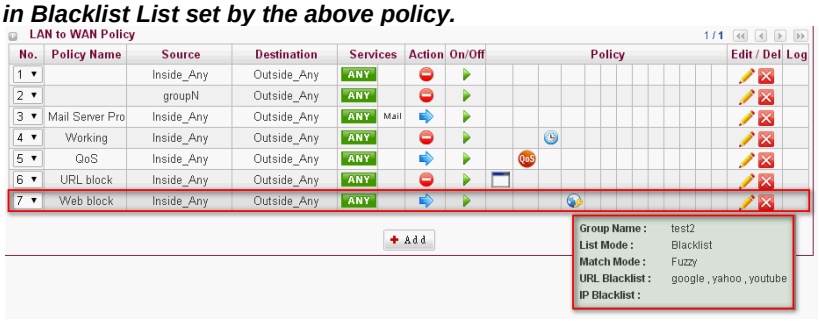
Example

Here is an example showing how URL Filter is used.

1. ***Select Policy > LAN Policy. Then select the function you need on the right side.***
2. ***Click on*** Add ***first and set Action to "Permit", and then select URL Access Control which you have previously set in section 6.6 URL Filter.***

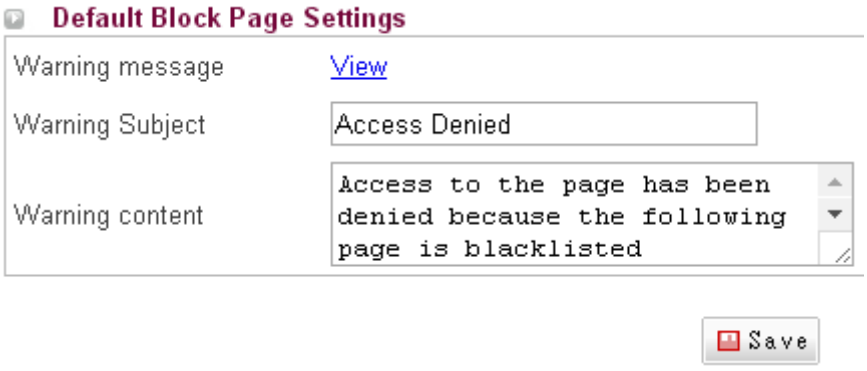


3. ***Setting URL Policy completed. User can browse websites except "youtube," "google," and "yahoo" which are restricted domain names in Blacklist List set by the above policy.***



6.6.3 Other Settings

Select *Objects* > *URL Filter* > *Other Settings*. It's a default block page settings.



6.7 Virtual Server

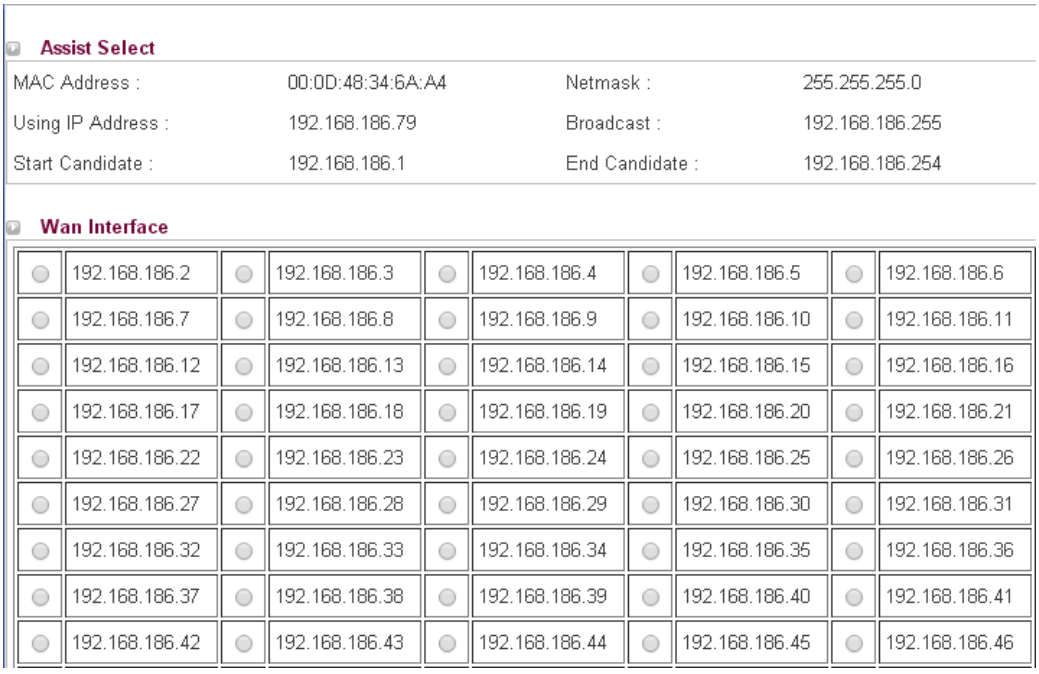
The real IP address provided from ISP is always not enough for all users when the system manager applies the network connection from ISP. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through IFW320's NAT (Network Address Translation) function. If a server that provides service to WAN network is located in LAN networks, external users cannot directly connect to the server by using the server's private IP address. The Virtual Server has set the real IP address of the IFW320's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the IFW320 translates the Virtual Server's IP address into the private IP address in the LAN network. Virtual Server owns another feature known as one-to-many mapping. This is when one real server IP address on the WAN interface can be mapped into many LAN network servers to provide the same service private IP addresses. This section covers the functionality and application of Virtual Server and Mapped IP. In this Virtual Server section you can enable the following lists:

6.7.1 Virtual Server

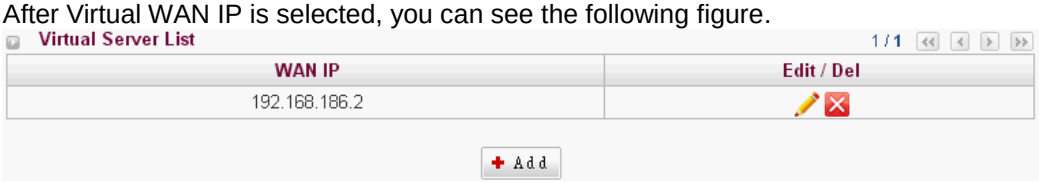
Its function resembles Mapped IP's. But the Virtual Server maps one-to-many. That is, to map a Real IP Address to LAN Private IP Address and provide the service item in Service. Select *Objects* > *Virtual Server*> *Virtual Server*. Click on Add button to create a new virtual server.

Click on Assist

Select IP address. It offers WAN Interface. Here, we suggest that you use "static IP."

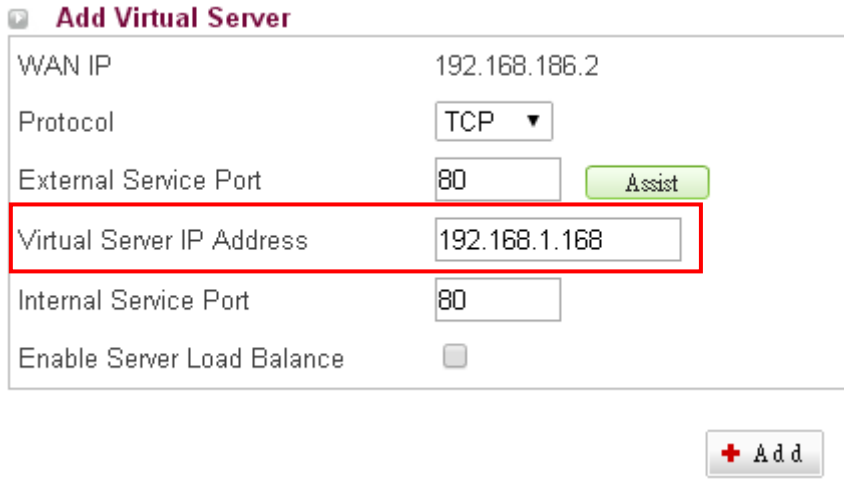


After Virtual WAN IP is selected, you can see the following figure.

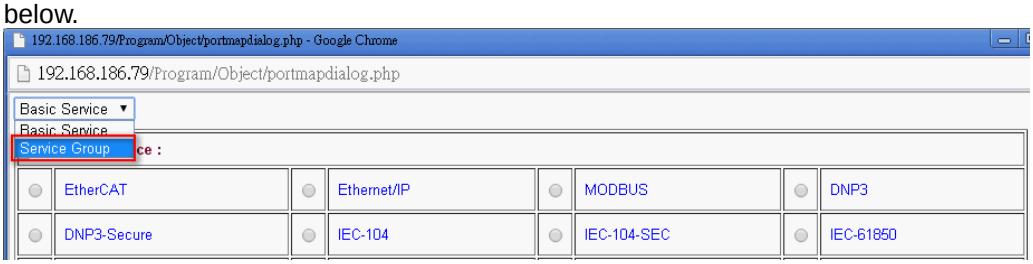


Setting Virtual Server WAN IP completed, you can see the following figure.

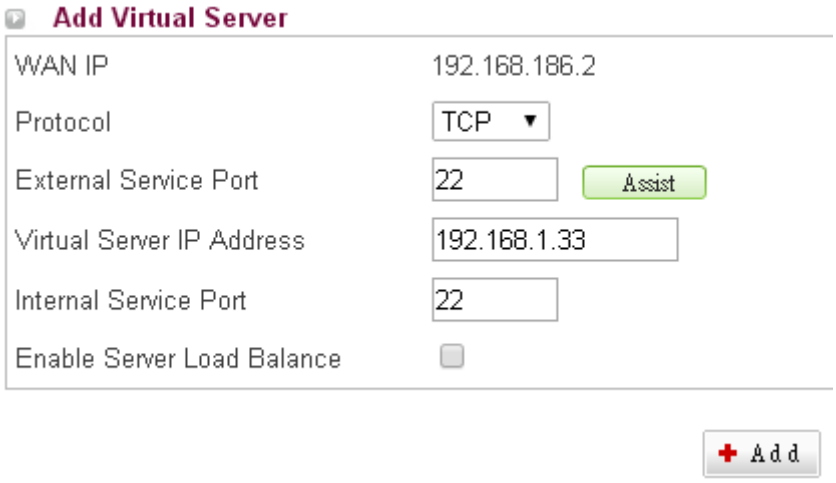
Click on to edit contents and click on to create a new Virtual Server IP Address.



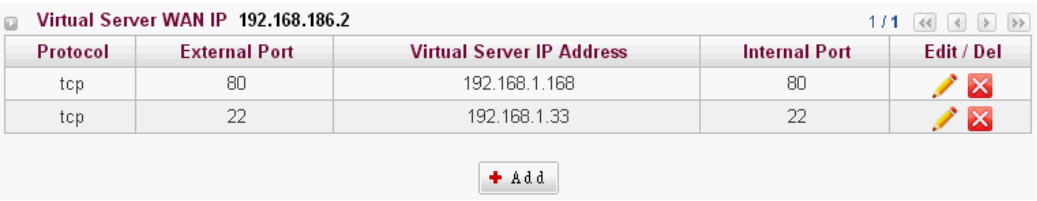
User can click on to select External Service Port easily as indicated in figure below.



Or enter a single port:

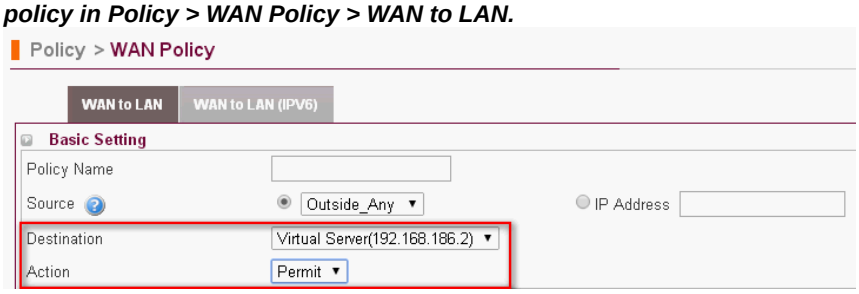


Setting Virtual Server completed. In addition, click on Add to create a new sub-content, to modify contents, or to cancel list.

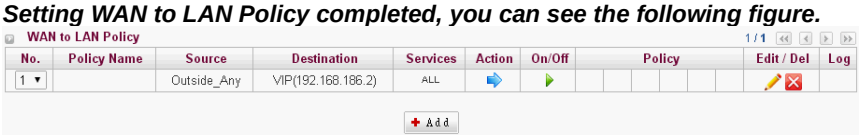


Example

Here is an example showing how to open mail server port in order to enable connection from outside user. Assume your Mail Server IP is 192.168.99.250. Please follow the previous steps, and then create a WAN policy in Policy > WAN Policy > WAN to LAN.



Setting WAN to LAN Policy completed, you can see the following figure.



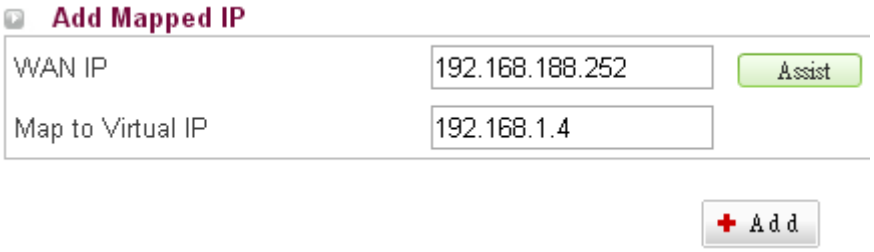
Then enter WAN IP and port number. For example, http://111.252.76.144:88. Figure below shows WAN Virtual Server 88 port.

Otherwise, enter WAN IP and port number, https://111.252.76.144:888. Figure below shows WAN Virtual 888 port

6.7.2 Mapped IP

Because of the intranet is transferring the private IP by NAT (NAT = Network Address Translation) Mode, so, NAT is used to map a WAN Real IP address to a LAN Private IP address. It is a one-to-one mapping. That is, to gain access to internal servers with private IP addresses from an external network, mapping is required.

Select *Objects* > *Virtual Server* > *Mapped IP.*

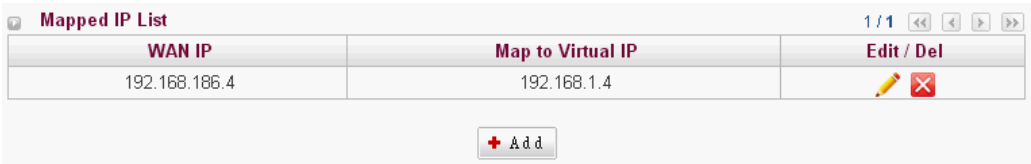


Click on to create a new one.

Click on
Click on this button for WAN IP address.

Map to Virtual IP
Create a Virtual IP for mapping.

Setting Mapped IP completed. In addition, click on to create a new sub-content, to modify contents, or to cancel list.

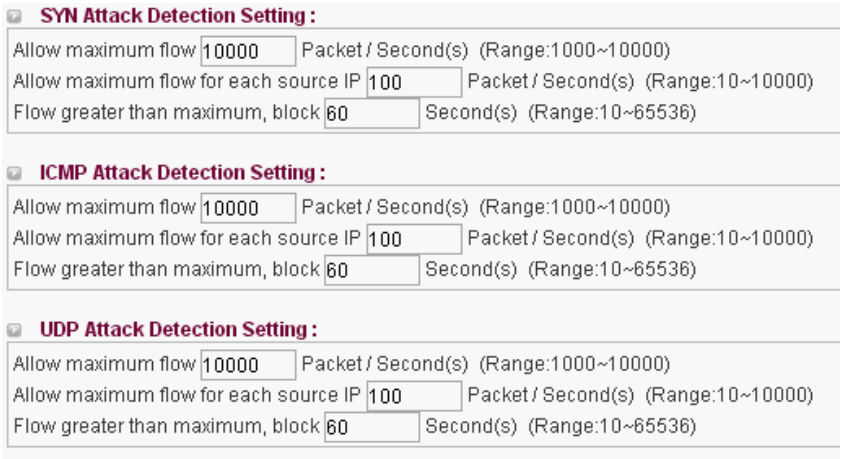


6.8 Firewall Protection

This section allows setting up the rules that specify if and how IP traffic flows through your IFW320 appliance. It offers a standard firewall and creates its firewall rules using firewall function. In this section you can enable the following lists:

6.8.1 Firewall Protection

Default firewall function status is “Start”. Select *Objects* > *Firewall Protection* > *Firewall Protection.*


SYN Attack Detection Setting :
Allow maximum flow 10000 Packet / Second(s) (Range:1000~10000)
Allow maximum flow for each source IP 100 Packet / Second(s) (Range:10~10000)
Flow greater than maximum, block 60 Second(s) (Range:10~65536)
ICMP Attack Detection Setting :
Allow maximum flow 10000 Packet / Second(s) (Range:1000~10000)
Allow maximum flow for each source IP 100 Packet / Second(s) (Range:10~10000)
Flow greater than maximum, block 60 Second(s) (Range:10~65536)
UDP Attack Detection Setting :
Allow maximum flow 10000 Packet / Second(s) (Range:1000~10000)
Allow maximum flow for each source IP 100 Packet / Second(s) (Range:10~10000)
Flow greater than maximum, block 60 Second(s) (Range:10~65536)

SYN Attack Detection Setting
SYN Flood is a popular attack way. DoS and DDoS are TCP protocol. Hackers like using this method to make a counterfeit of connection; and the CPU, memory and so on resources are consumed.

ICMP Attack Detection Setting
ICMP is kind of a pack of TCP/IP; its important function is for transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.

UDP Attack Detection Setting
Hackers use UDP Protocol to make a counterfeit of connection, and the CPU, memory and so on resources are consumed.

Source IP address block
Please enter source IP address that needs to be blocked.

Destination IP address block
Please enter destination IP address that needs to be blocked.

Other Items
In addition to SYN attack detection, ICMP attack detection, and UDP attack detection, IT administrators can check to choose from various detections provided.

6.8.2 Attack Log

Select *Objects* > *Firewall Protection* > *Attack Log*. You can see all of attack detection records which go through IFW320 machine, see figure below.

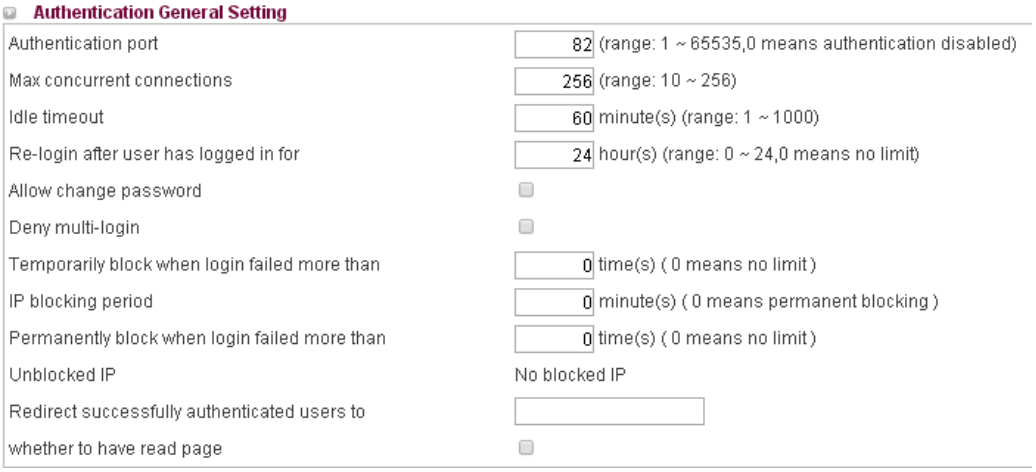
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255
2013-09-10 14:03:31	UDP Attack	UDP	137	WAN1	192.168.1.15	192.168.1.255

6.9 Authentication

Internet Authentication serves as a gateway to filter out unauthorized users from accessing the Internet. Configuring the Authentication provides an effective method of managing the network's use. Therefore, IT administration can control the user's connection authority by setting account and password to identify the privilege, and then users have to pass the authentication to access to Internet. In this section, it offers some authentication modes, Local Users, User Group, External Authentication Settings including AD (AD = Active Directory) and POP3 to add flexibility to your choice of authentication method. In addition, it also offers Internet Authentication Recorder and Authentication Status. The IT administrator can use two methods to know the authentication of LAN's users and what they have been done. In this Authentication section you can enable the following lists:

6.9.1 Auth Setting

Select *Objects* > *Authentication* > *Auth Setting.* Figure below shows Authentication common settings.


Authentication General Setting
Authentication port
82 (range: 1 ~ 65535,0 means authentication disabled)
Max concurrent connections
256 (range: 10 ~ 256)
Idle timeout
60 minute(s) (range: 1 ~ 1000)
Re-login after user has logged in for
24 hour(s) (range: 0 ~ 24,0 means no limit)
Allow change password
Deny multi-login
Temporarily block when login failed more than
0 time(s) (0 means no limit)
IP blocking period
0 minute(s) (0 means permanent blocking)
Permanently block when login failed more than
0 time(s) (0 means no limit)
Unblocked IP
No blocked IP
Redirect successfully authenticated users to
whether to have read page

Authentication port
The port number that authentication requires. Default port is 82.

Idle timeout
If an authenticated connection has been idle for a period of time, it will expire. The default idle timeout is 60 minutes.

Re-login after user has logged in for
After user logged in for a period of time, a re-registration will be requested. Determine the valid time of an authentication. Authentication expires on the due time.

Allow change password
Permit users who are using the device's local authentication mechanism to modify their own password.

Deny multi-login
When enabled, once a user has logged in with his/her authentication account, no other user is permitted to log into the same account.

Temporarily block when login failed more than
Perform temporary blocking when login failures exceed the number of time(s) entered in this field.

Caution ***0 means no limits.***

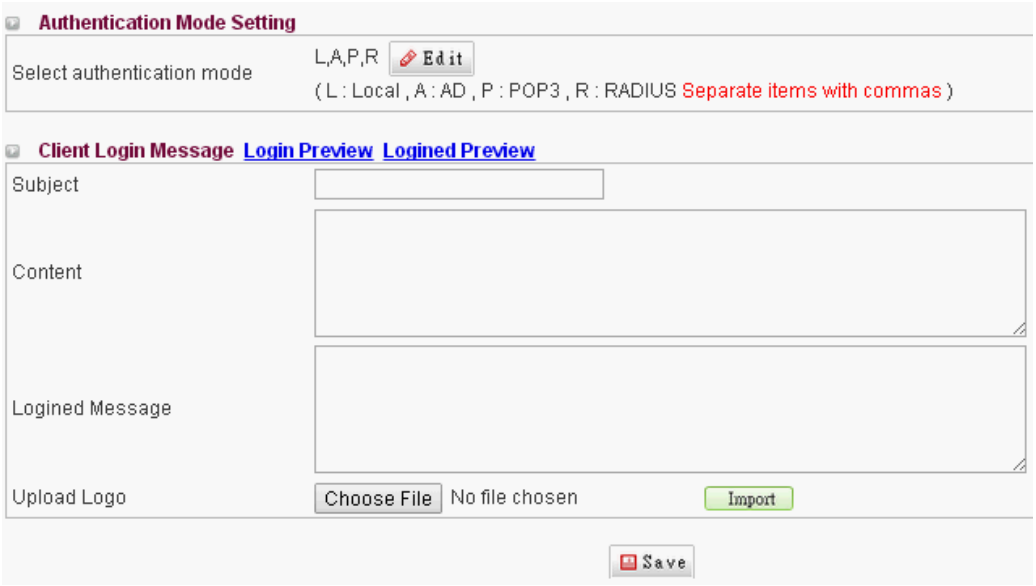
IP blocking period
Determine the amount of time for blocking the corresponding IP.

Caution ***0 means permanent blocking.***

Permanently block when login failed more than
Perform permanent blocking when login failures exceed the number of time(s) entered in this field.

Caution ***0 means no limits.***

Redirect successfully authenticated users to
Authenticated user can be redirected to the designated website by assigning its address to this field. Leaving it blank means the user will just go directly to their desired website.



Select Authentication Mode
Click on Edit button to enter mode. These modes are separated by using comma.

1. L: Local
2. A: AD
3. P: POP3

Subject
Enter some words for website subject.

Content
Enter some messages for showing in the login screen. Leaving it blank will result in no message being shown.

Upload logo
Click on “Choose File” to select logo file. After selected, click on Import. This picture will show when users use Internet through this Internet Authentication. The Login screen shows before user accesses a website.

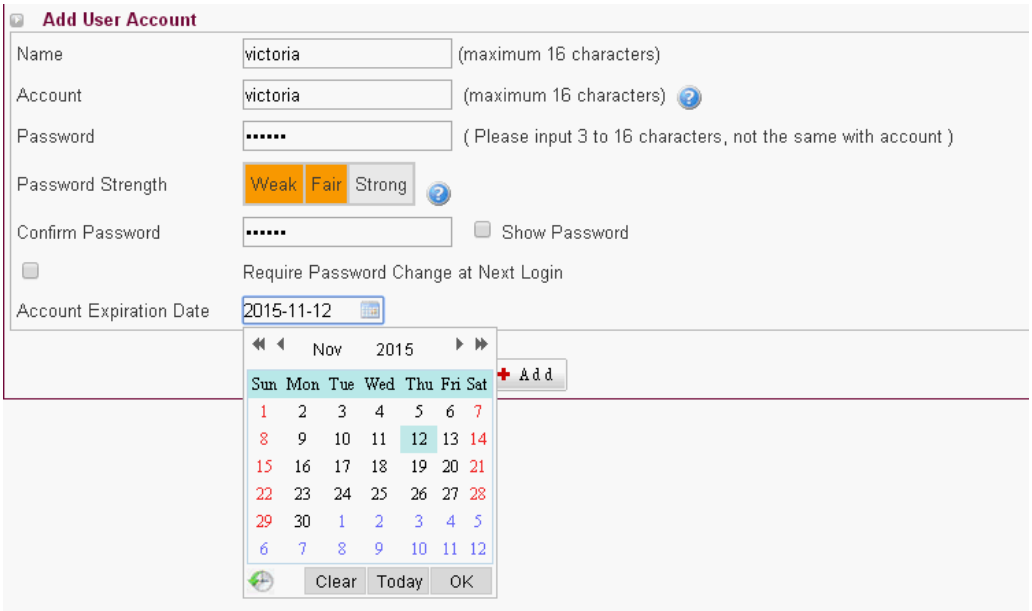
You can click on “Login Preview” to preview login screen, see an example screen in figure below.

6.9.2 Local User

Select *Objects > Authentication > Local User.*

User List
If you have many accounts, you can click on Browse... to bring in accounts. After selected, click on Import. Then, you do not have to enter account step by step.

Click on + Add first.



Name
The user name for authentication.

User Account
The account for authentication.

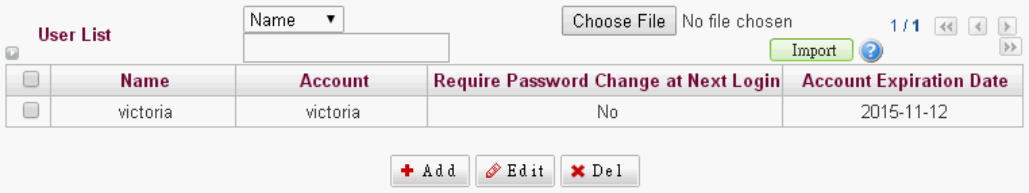
Password
The password for authentication.

Confirm Password
The confirmation of password.

Require Password Change at Next Login
If selected, the local authentication accounts can be forced to change their passwords at their next login attempt.

User account expiration date
Set the period of validity for a user's account

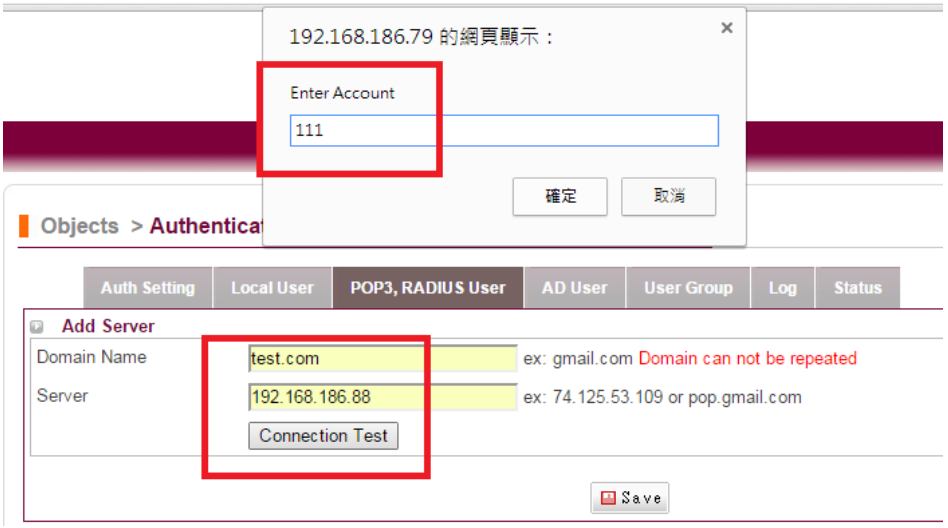
Setting Local Users completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.



And then, please refer to User Group section to learn how to use Internet Authentication.

6.9.3 POP3, RADIUS User

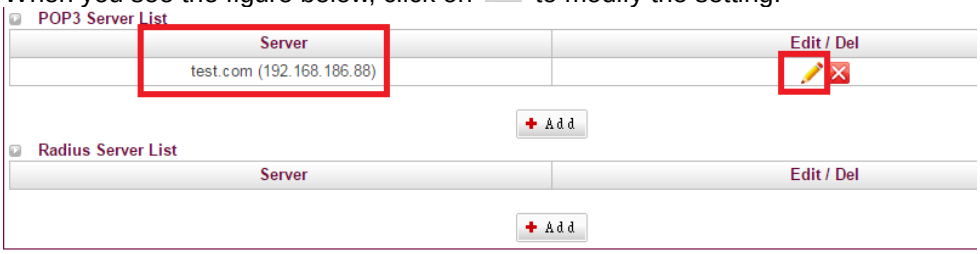
Select *Objects* > *Authentication* > *RADIUS User.* Enter domain name and IP address of your mail server, then check on connection. Please enter an account and password of the mail server for connection test, see figure below.



If the info is correct, it will display “Login Test Success” (see figure below).

If the info is incorrect, it will display “Login Test Failed”, see figure below. If this happens, please check the accuracy of the information provided.

When you see the figure below, click on to modify the setting.



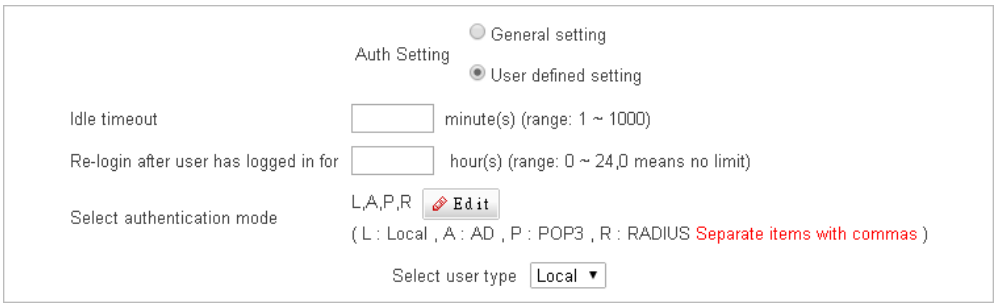
After editing the setting, you may add email account(s) at “Server Member Setting” below.

6.9.4 User Group

Select *Objects* > *Authentication* > *User Group.*

Click on **.**

Group name
Enter some words for recognition.

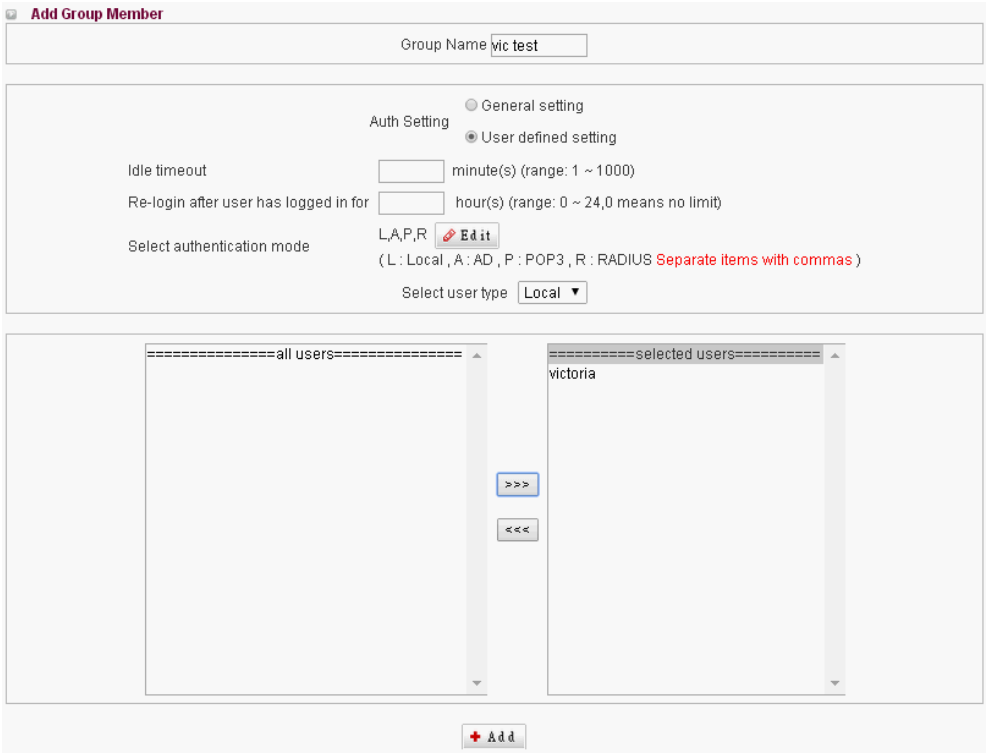

Auth Setting
General setting
User defined setting
Idle timeout
minute(s) (range: 1 ~ 1000)
Re-login after user has logged in for
hour(s) (range: 0 ~ 24,0 means no limit)
Select authentication mode
L,A,P,R
Edit
(L : Local , A : AD , P : POP3 , R : RADIUS Separate items with commas)
Select user type
Local

Auth Setting

1. General setting: It accords with Auth Settings.
2. User defined setting: The settings of Idle timeout, Re-login after user has logged in for, and Select Authentication Mode are defined by yourself.

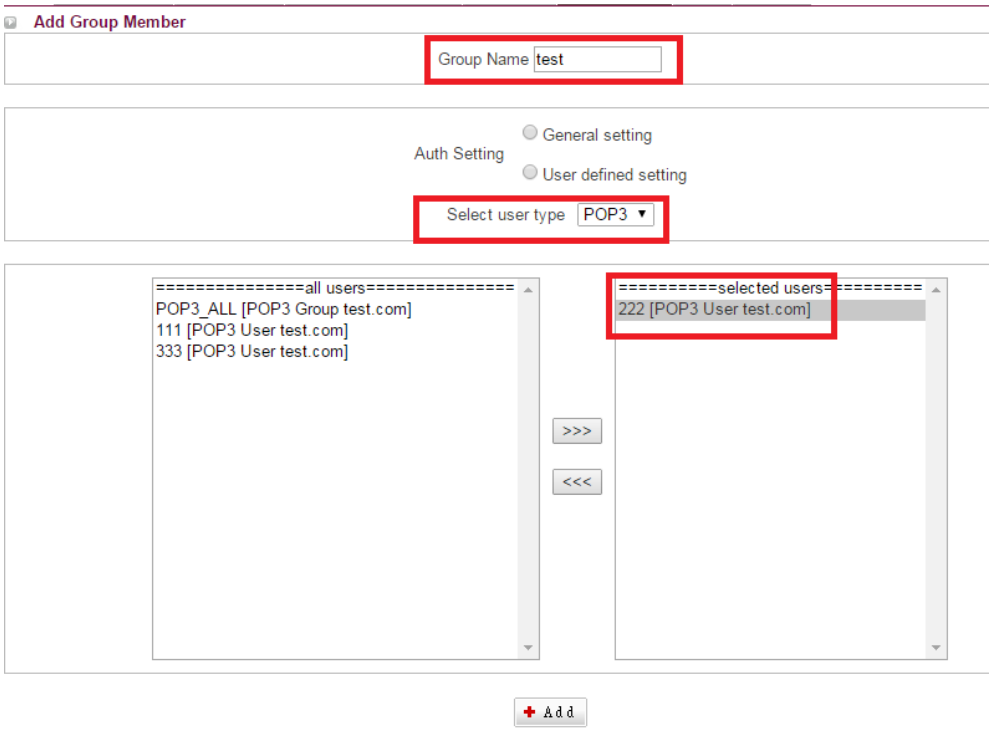
Select user type
There are two choices.

1. This machine (Local Users)

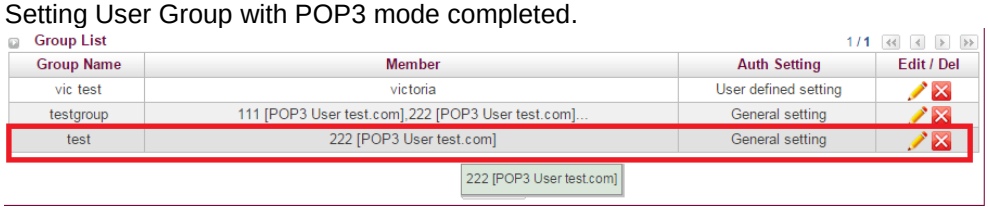


Setting User Group with Local Users mode completed. In addition, click on Add to create a new sub-content, to modify contents, or to cancel list.

2. POP3.
   Enter a group name, choose POP3 for user type. And move the accounts from the left to the right. Accounts can be a single account or a group of POP accounts.

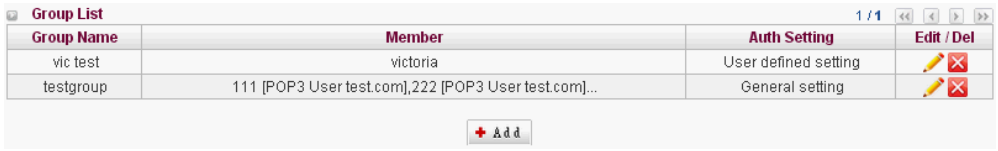


Setting User Group with POP3 mode completed.



In addition, click on

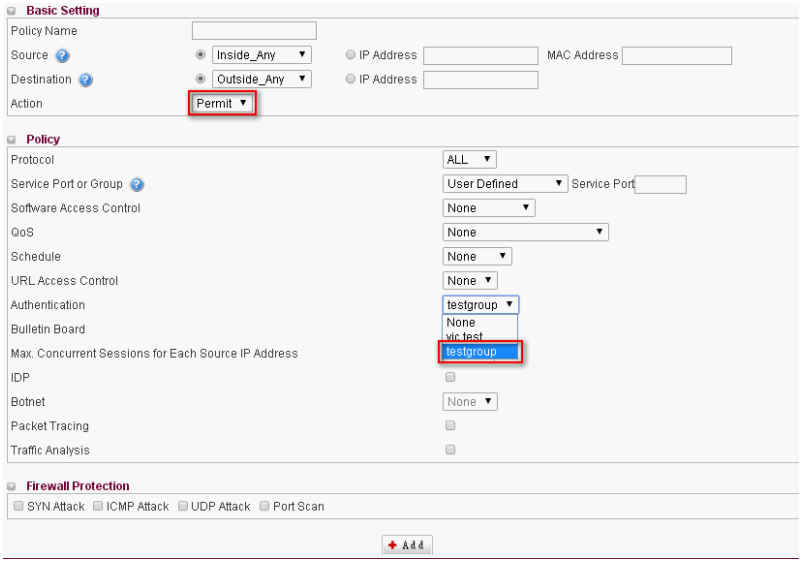
to create a new sub-content, to modify contents, or to cancel list.



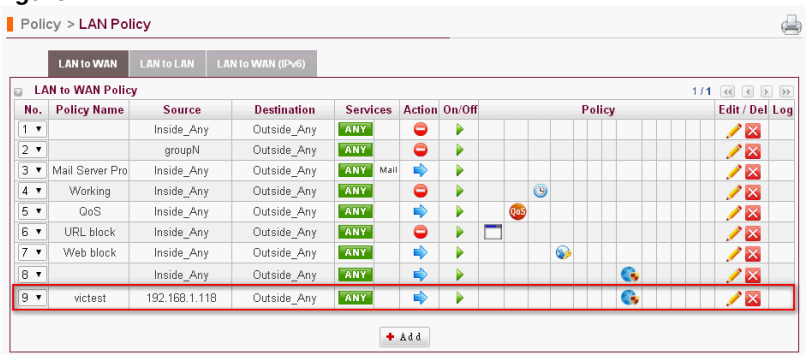
Example

Here is an example showing how User Group with Local User mode is used.

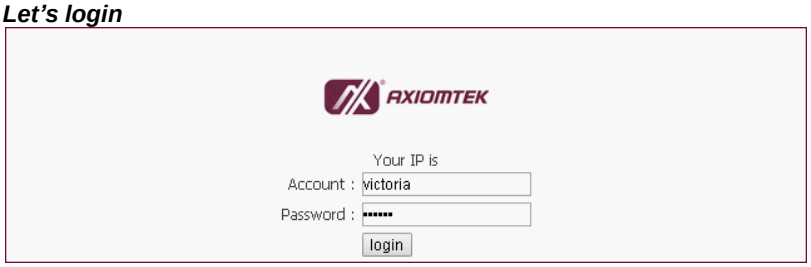
1. ***Select Objects > Policy > LAN Policy. Then select the function you need on the right side.***
2. ***Click on*** Add ***and set Action to "Permit", and then set Authentication to "vic test" which you have previously set in section 6.9 Authentication.***



3. ***Setting Authentication Policy completed, you can see the following figure.***



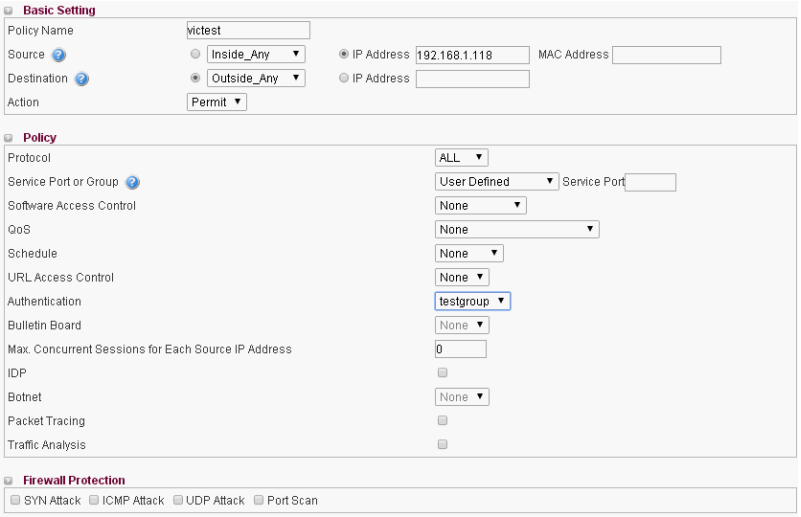
4. ***Let's login***



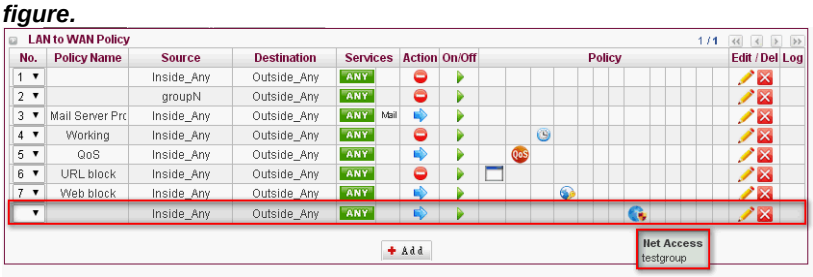
Example

Here is an example showing how User Group with POP3 mode is used.

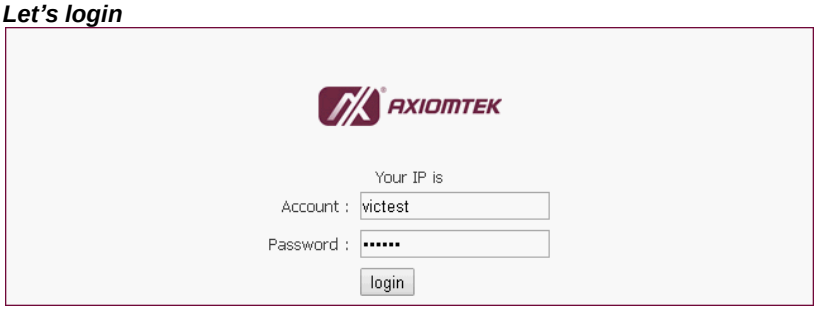
1. ***Select Objects > Policy > LAN Policy. Then select the function you need on the right side.***
2. ***Click on*** ***and set Action to "Permit", and then set Authentication to "testgroup" which you have previously set in section 6.9 Authentication.***



3. ***Setting Authentication Policy completed, you can see the following figure.***

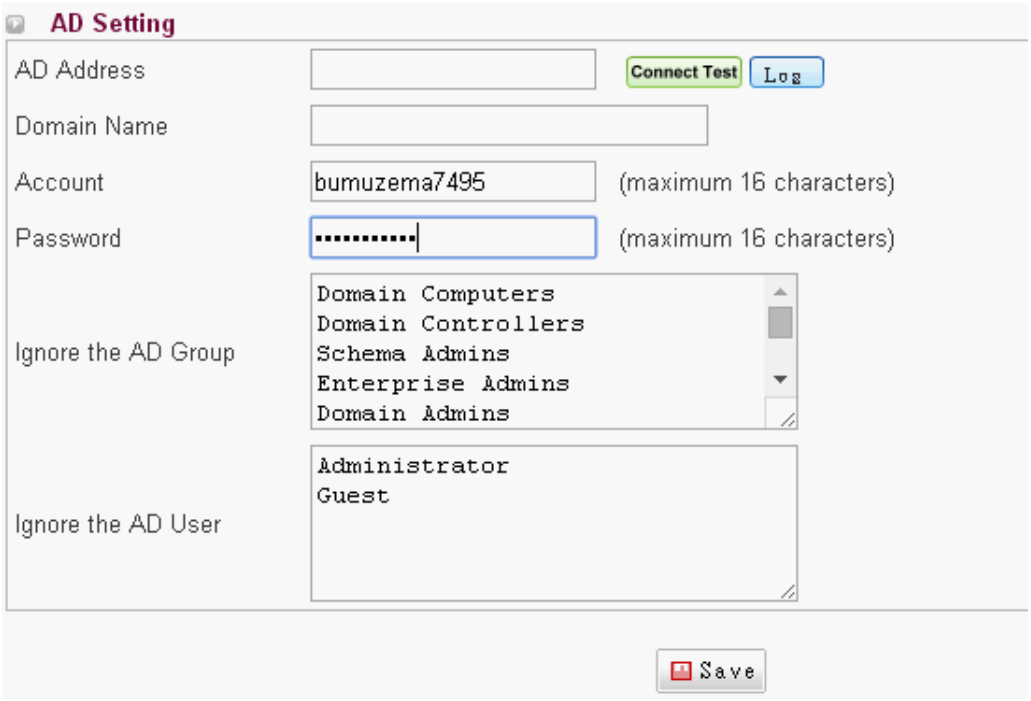


4. ***Let's login***



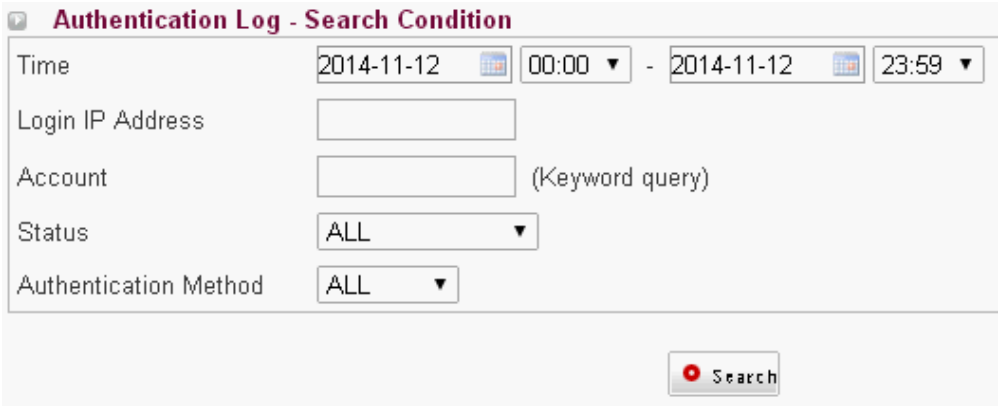
6.9.5 AD User

Select *Objects* > *Authentication* > *AD User.* Enter your AD server information and click on Connect Test first to make sure whether it is correct or not. Then, click on Save.



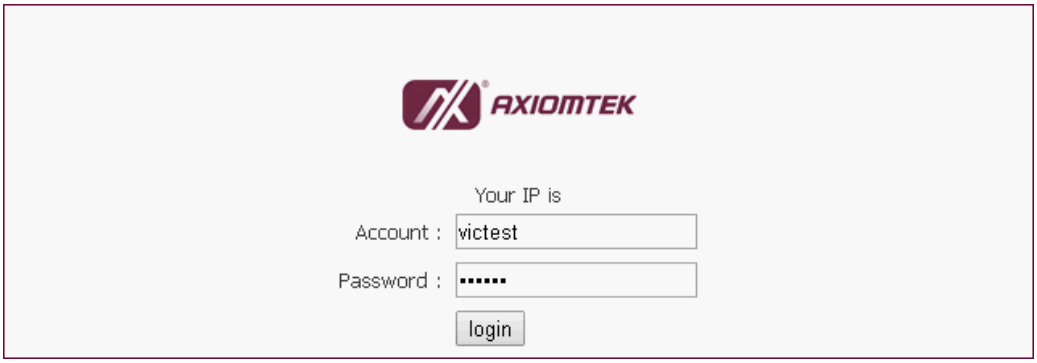
6.9.6 Log

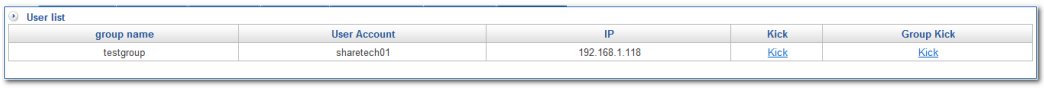
This function accords with previous sections such as Authentication Settings, Local Users and User Group sections. If the user has login, the records will be shown.



6.9.7 Status

It shows the users who are on the Internet at present. You can click on “Kick” link to kick out the user or user group for not letting them to use the Internet.





6.10 Bulletin Board

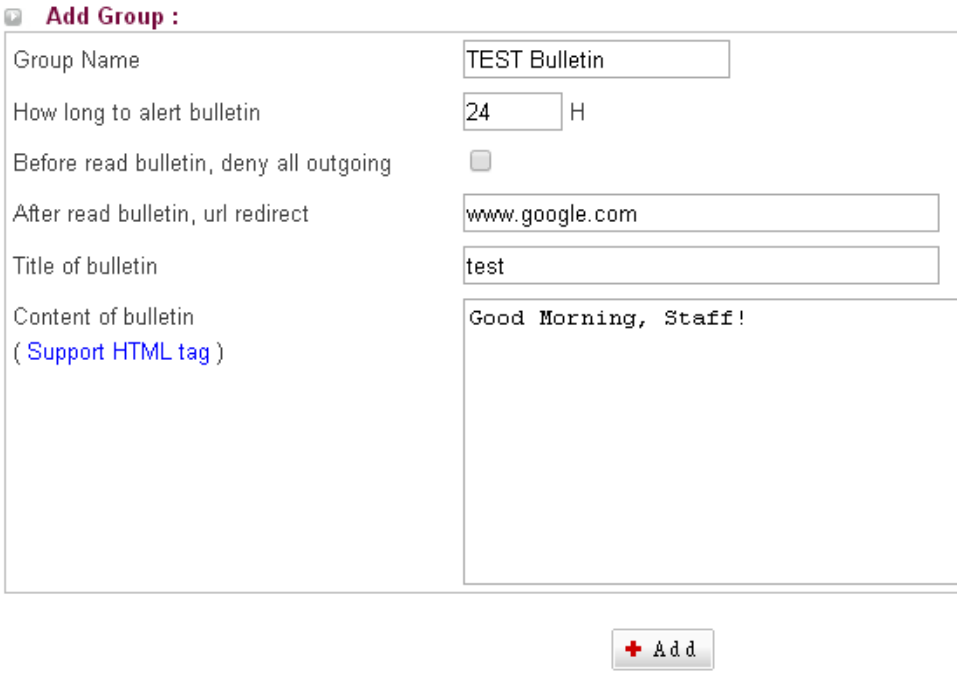
In a workplace environment, bulletin boards can save time, promote productivity and efficiency. The bulletin board offered as part of a company's internal extranet communication systems saves people the hassle of sorting through superfluous emails that aren't work-related. Instead, assignments, memos and messages from clients can be posted on the company's bulletin board.

Caution

Bulletin Board and Authentication cannot be used together.

6.10.1 Bulletin Setting

Select *Objects* > *Bulletin Board* > *Bulletin setting*. Click on + Add to add new bulletin board.



Group Name
Enter any words for recognition.

How long to alert bulletin
Please enter 0~24 hours.

Before read bulletin, deny all outing
Internal users cannot surf Internet if users do not read content of bulletin yet.

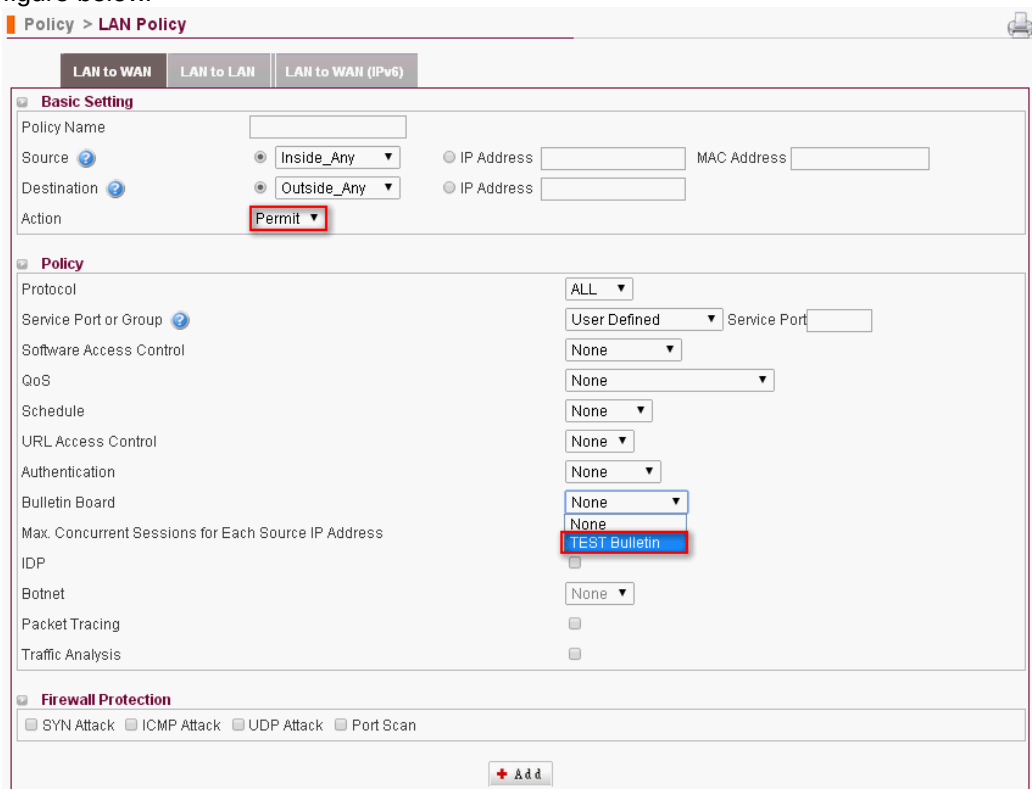
After read bulletin, url redirect
After bulletin is read, user will be redirected to URL address set in this field.

Title of bulletin
Enter any words for your title name.

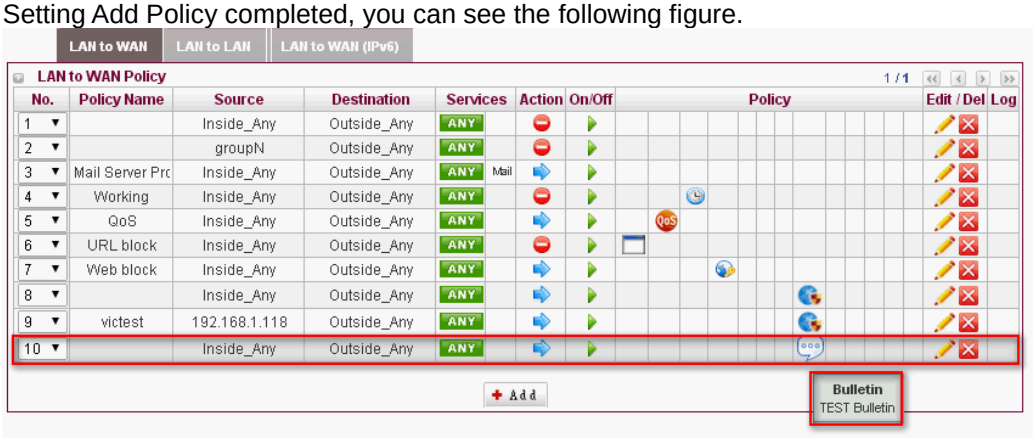
Content of bulletin
Enter some messages for showing in bulletin board.

Setting Local Users completed. In addition, click on + Add to create a new sub-content, Edit to modify contents, or Del to cancel list.

Then, select *Policy* > *LAN Policy* > *LAN to WAN*. Click on + Add to add new policy, see figure below.

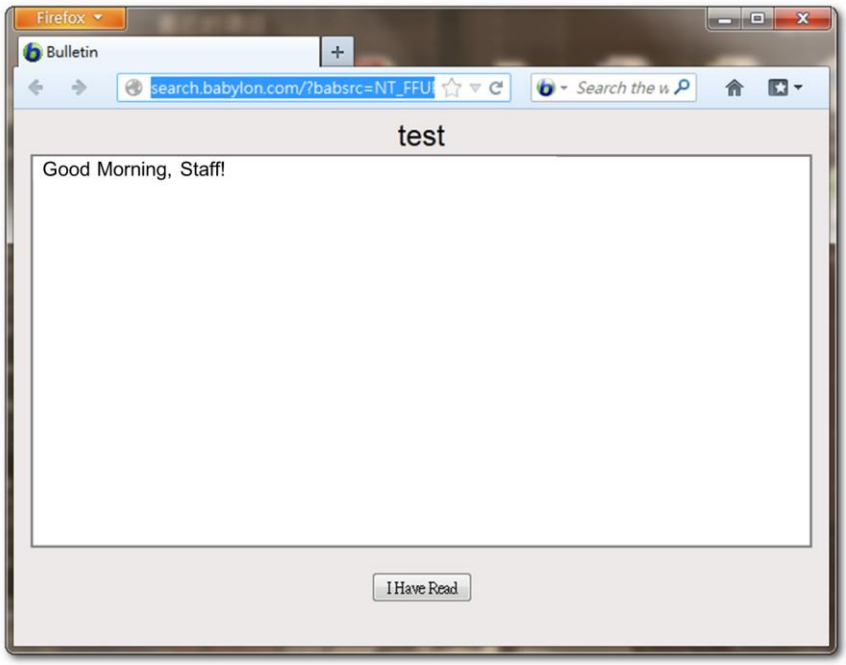


Setting Add Policy completed, you can see the following figure.

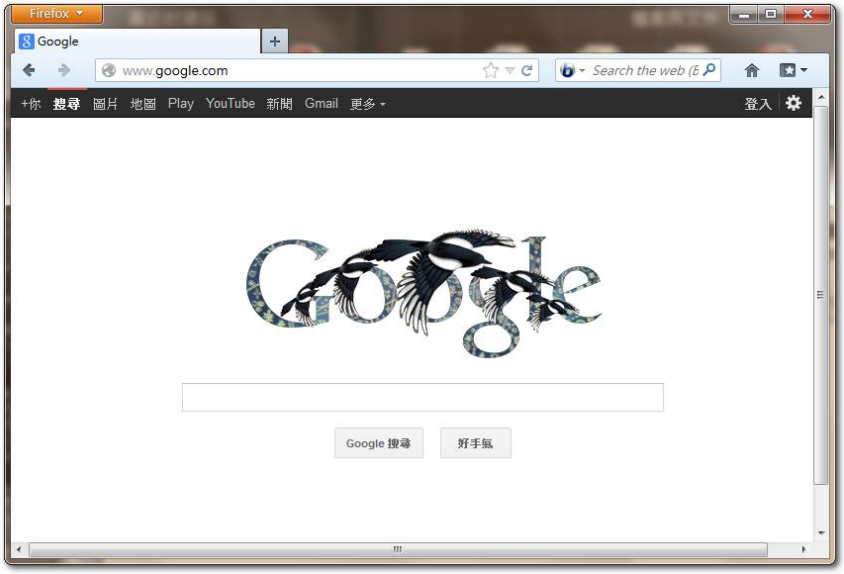


Example

The internal users will see bulletin board when they use web browser, see figure below.

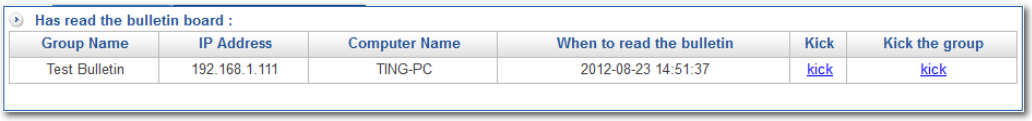


After users read bulletin content and click on ***, URL redirect to website Administrator enter.***



6.10.2 Has Read the Bulletin Board

Select *Objects* > *Bulletin Board* > *Has read the bulletin board*.


Has read the bulletin board :

Group Name	IP Address	Computer Name	When to read the bulletin	Kick	Kick the group
Test Bulletin	192.168.1.111	TING-PC	2012-08-23 14:51:37	kick	kick

Administrator can see which IP had read content of bulletin board. Internal user has to read again if kicked out.

This page is intentionally left blank.

Chapter 7
Network Services

This chapter includes services used by the various proxies, such as DNS/DDNS/DHCP Services and High Availability. In the Network Services chapter you can enable the following lists:

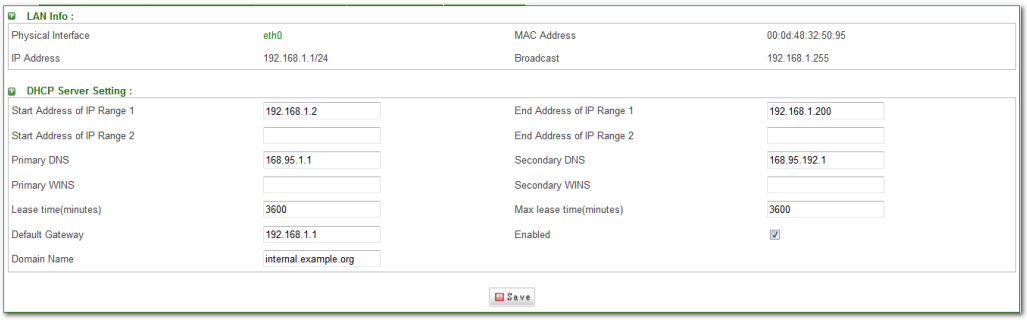
- DHCP
- DDNS
- DNS Proxy
- High Availability
- SNMP
- Remote Syslog Server

7.1 DHCP

The DHCP (DHCP = Dynamic Host Configuration Protocol) service allows you to control the IP address configuration of all your network devices from IFW320 appliance in a centralized way. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP, this is something called "automatic network configuration" and is often the default setting. You may choose to provide this service to clients on your LAN only, or include devices on WAN zone. In this section you can enable the following lists:

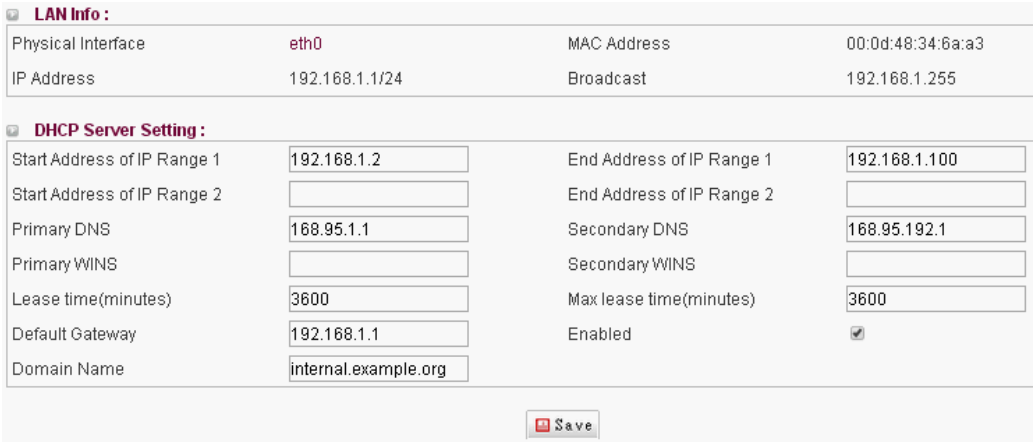
7.1.1 LAN User List

Select *Network Services > DHCP > LAN User List*.



7.1.2 LAN DHCP Server

Select *Network Services* > *DHCP* > *LAN DHCP Server*.



Start / End address of IP Range 1 and 2
Specify the range of addresses to be handed out. These addresses have to be within the subnet that has been assigned to the corresponding zone.

Primary / Secondary DNS
This specifies the DNS to be used by your clients. Since IFW320 appliance contains a caching DNS server, the default value is the firewall's own IP address in the respective zone.

Lease time (minutes)
This defines the default/maximum time in minutes before the IP assignment expires and the client is supposed to request a new lease from the DHCP server.

Max lease time (minutes)
In order to avoid IFW320 using the same IP, this is used to set maximum lease time we can establish for the same IP.

Default Gateway
The default gateway of the LAN.

Domain name
This is the default domain name that is passed to the clients. When the client looks up a hostname, it will first try to resolve the requested name. If that is not possible, the client will append this domain name preceded by a dot and try again.

7.1.3 DHCP Static IP

Select *Network Services* > *DHCP* > *DHCP Static IP*. In this section, if you have selected "Get static IP address from DHCP Server" tick box, you will see DHCP Static IP list here.

7.2 DDNS

DDNS (DDNS = Dynamic DNS), it allows you to make your server available to the Internet even though it does not have a static IP address. To use DDNS you must first register a sub-domain with a DDNS provider. Then whenever your server connects to the Internet and is given an IP address by your ISP it must tell the DDNS server this IP address. When a client machine wishes to connect to your server it will resolve the address by asking the DDNS server, which will answer with the latest value. If this is up to date then the client will be able to contact your server (assuming your firewall rules allow this). EFW makes the process of keeping your DDNS address up to date easier by providing automatic updates for many of the DDNS providers. In this section you can enable the following lists:

7.2.1 DDNS Server

Dynamic DNS provider includes a service that allows assigning a globally available domain name to IP addresses. This works even with addresses that are changing dynamically such as those offered by residential ADSL connections. For this to work, each time the IP address changes, the update must be actively propagated to the Dynamic DNS provider.

Select *Network Services* > *DDNS* > *DDNS Server.* Click on to create a new one.

Service Provider
Choose the DDNS provider.

Hostname
The hostname and domain as registered with your DDNS provider.

Example

For instance, "Axiomtek" and "dhs.org".

WAN
Select the WAN interface that the domain name corresponds to.

Account
Enter an account for DDNS server.

Password
Enter a password for DDNS server.

Comment
Enter any word for recognition.

Enabled
Select “Enabled” tick box. If it is not ticked, the Firewall will not update the information on the DDNS server. It will retain the information so that you can re-enable DDNS updates without reentering the data. It contains a DDNS client for 14 different providers - if it is enabled, it will automatically connect to the dynamic DNS provider and tell it the new IP address after every address change.

Setting DDNS Server completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list.

7.3 DNS Proxy

The Domain Name System (DNS) is a standard technology for managing the names of websites and other Internet domains. DNS technology allows you to type names into your web browser like *compnetworking.about.com* and your computer to automatically find that address on the Internet. A key element of the DNS is a worldwide collection of DNS servers.

A DNS server is any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

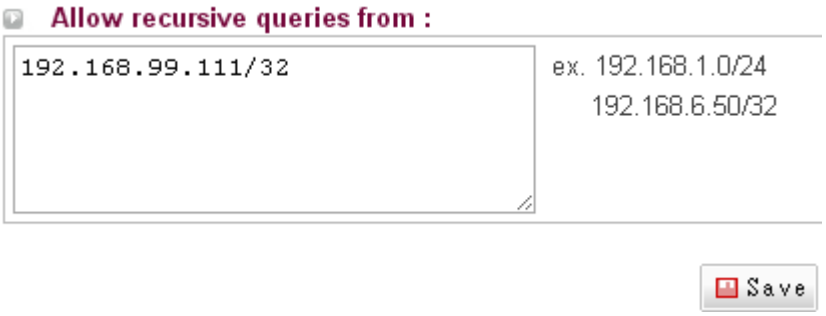
Example

For example, the domain names are translated to IP address. Therefore, "www.Axiomtek.com.tw" " might be translated to "211.22.160.28".

Actually, hostnames and IP addresses do not necessarily match on a one-to-one basis. Multiple hostnames may correspond to a single IP address: combined with virtual hosting, this allows a single machine to serve many websites. Alternatively a single hostname may correspond to many IP addresses: this can facilitate fault tolerance and load distribution, and also allows a site to move physical location seamlessly. In this section you can enable the following lists:

7.3.1 General Setting

Enter internal IP range in order to help them query domain name.



7.4 High Availability

IFW-320 can be easily run in HA (HA = High Availability) mode. At least two IFW320 machines are required for HA mode: one assumes the role of the active (Master) firewall while the others are standby (Backup) firewalls. If the Master firewall fails, an election between the Backup will take place and one of them will be promoted to the new Master, providing for transparent failover. In this section you can enable the following lists:

7.4.1 High Availability

To set up such a HA configuration, first set up the firewall that is going to be the Master. At this point the Backup mode cannot be reached anymore via its old IP address (factory default or previous LAN address).

1. Select *Network Services* > *High Availability* > *High Availability*.
2. Select “Enable” tick box to start function, and set mode to “Master”.
3. The Manage IP is the first IP address of the management network.
4. The Remote IP is the special subnet to which all IFW320 that are part of a HA setup must be connected via the LAN interface.
5. Finally, click on

to activate the settings.

Setup the firewall that is going to be the backup. At this point an extra panel appears where the Backup-specific settings can be configured.

1. Execute the setup wizard, including the network wizard, filling in all needed information. It is not necessary to configure services, etc., since this information will be synchronized from the master. However, it is necessary to register the backup with Axiomtek network.
2. Select *Network Services* > *High Availability* > *High Availability*.
3. Enable: Select “Enable tick” box to start function, and set mode to Backup.
4. Fill in the Manage IP management network address for the Backup.
5. Fill in the Remote IP (the Backup needs this to synchronize its configuration from the Master).
6. Finally, click on

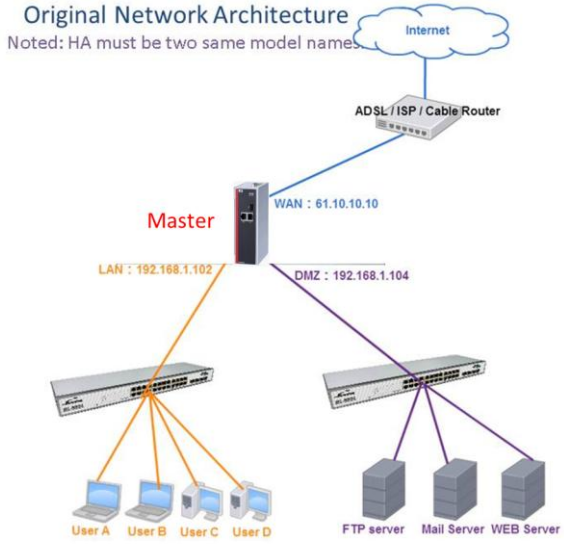
to activate the settings

In conclusion, the Backup mode cannot be reached anymore via its old IP address (factory default or previous LAN address) since it is in standby mode. It is connected to the Master mode only through the management network.

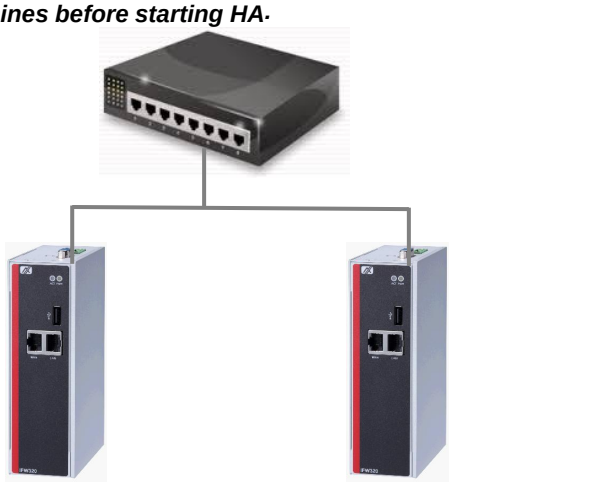
Example

Here is an example for your reference.

1. ***First of all, check the original network architecture.***



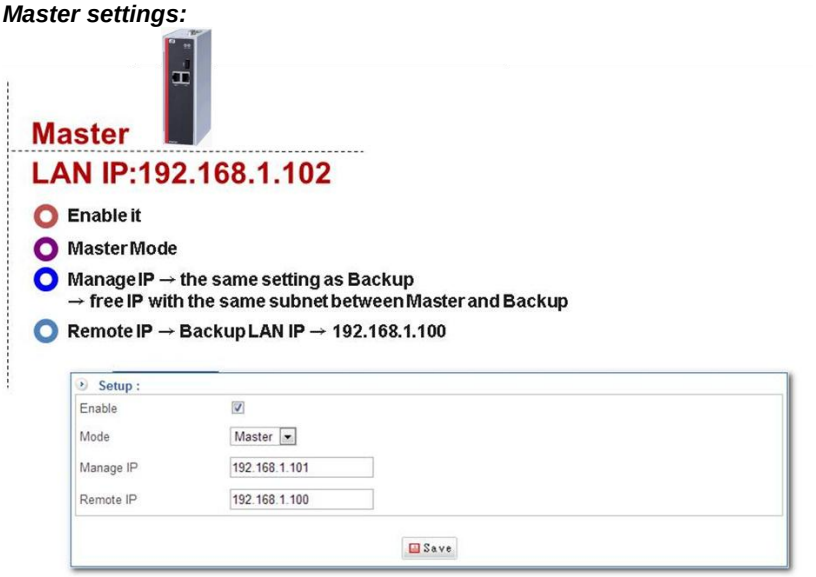
2. ***Install machines before starting HA.***



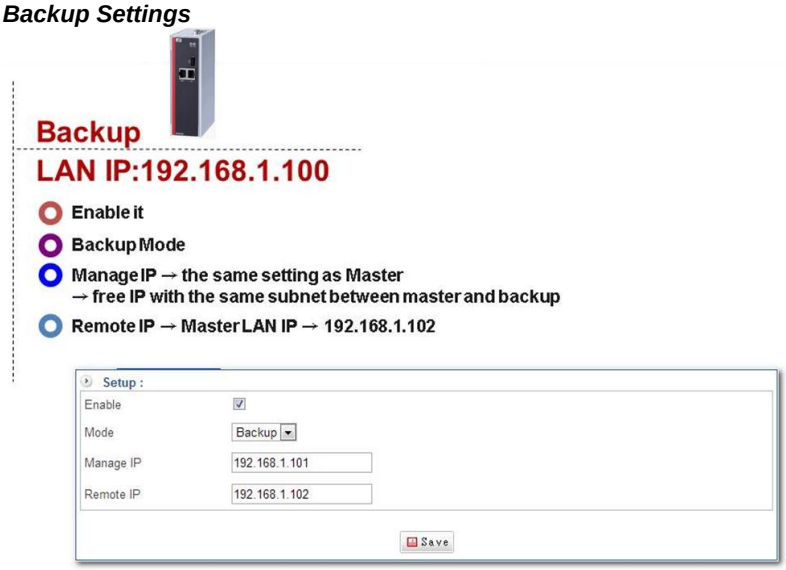
Master
LAN IP: 192.168.1.102

Backup
LAN IP: 192.168.1.100

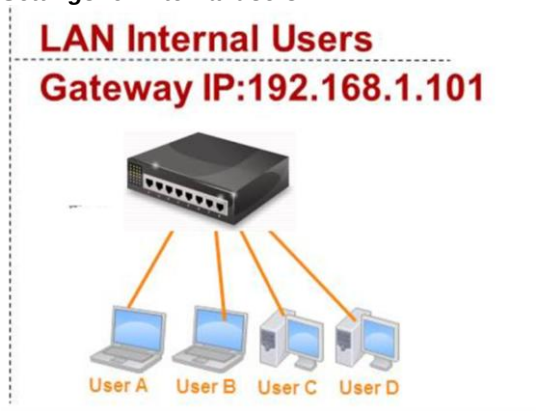
3. Master settings:



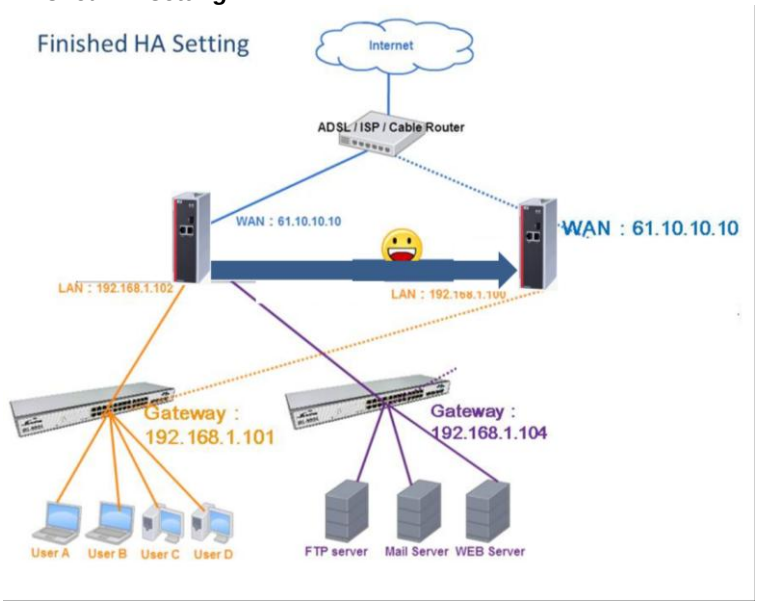
4. Backup Settings



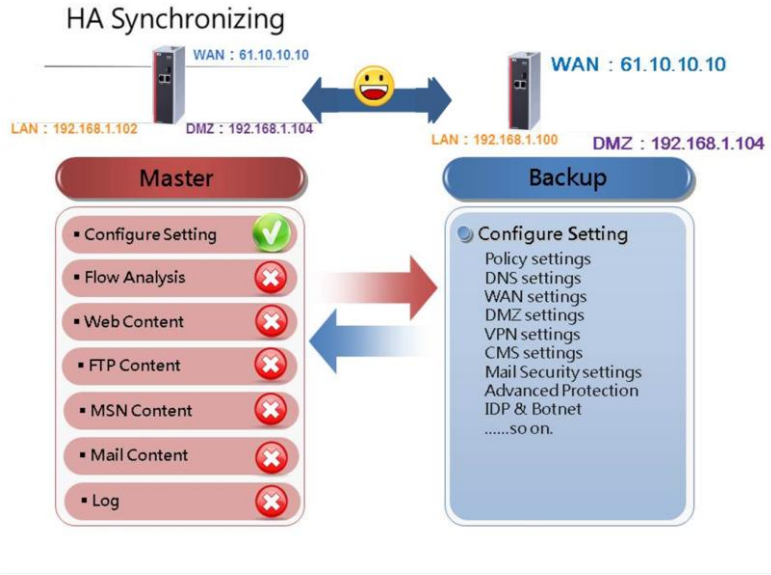
5. Settings for internal users:



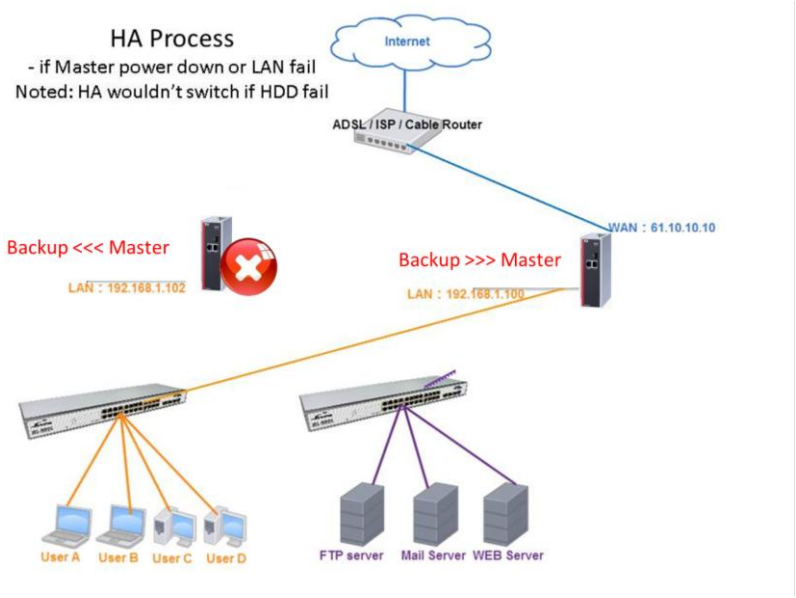
6. Finished HA setting:



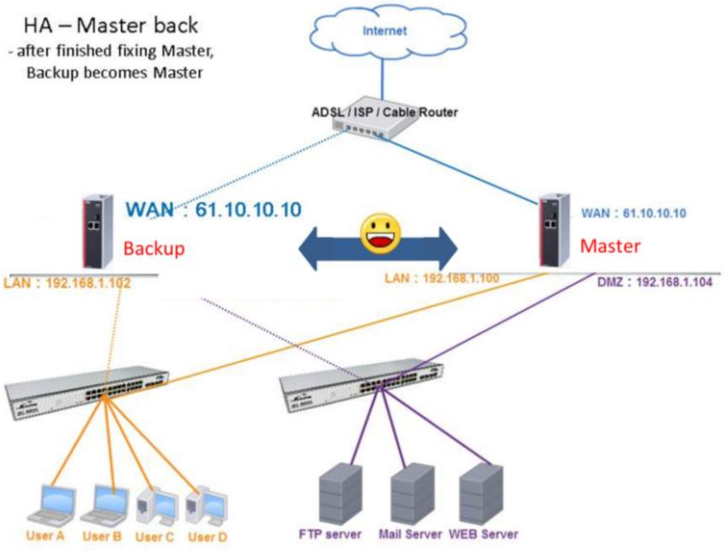
7. HA Synchronizing:



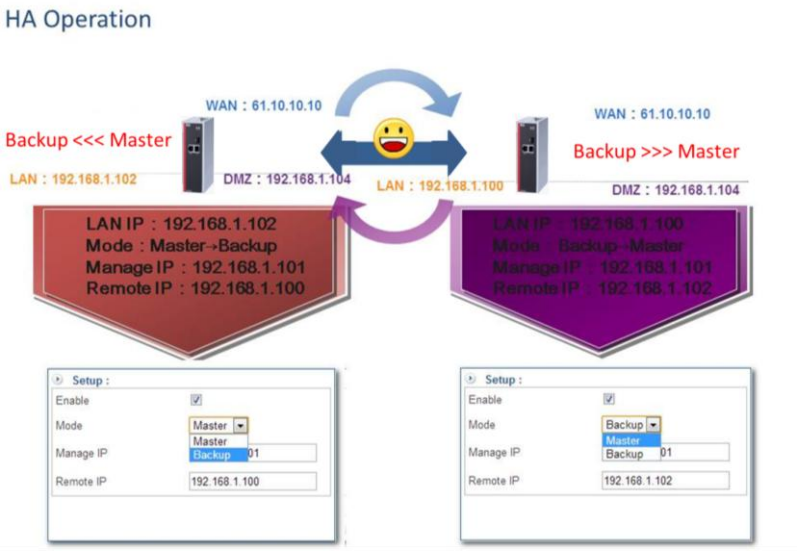
8. ***If Master is broken, Backup will take over network and becomes Master.***



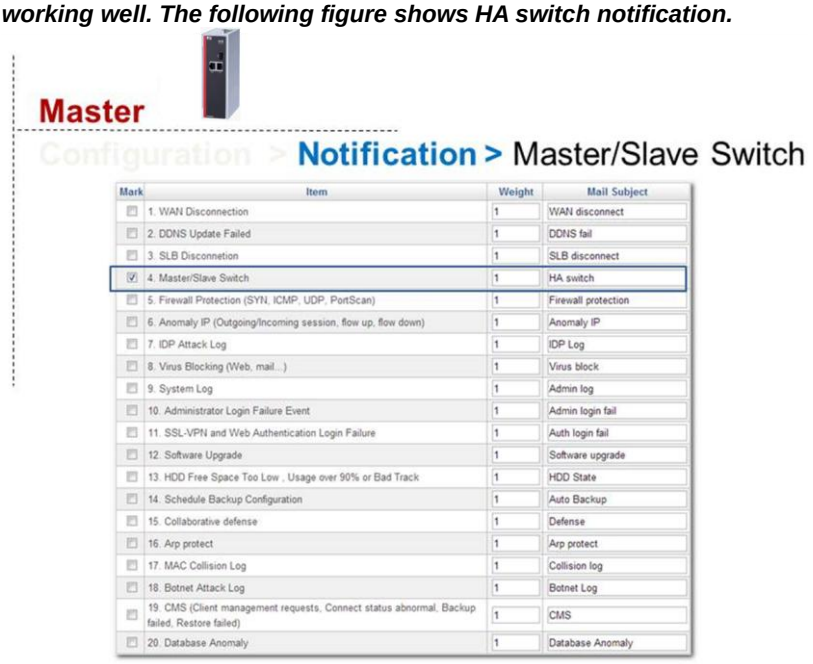
9. ***When the original Master is fixed and back again, it becomes Backup.***



10. HA operation:



11. Besides, you can enable notification if you worry about the system not working well. The following figure shows HA switch notification.

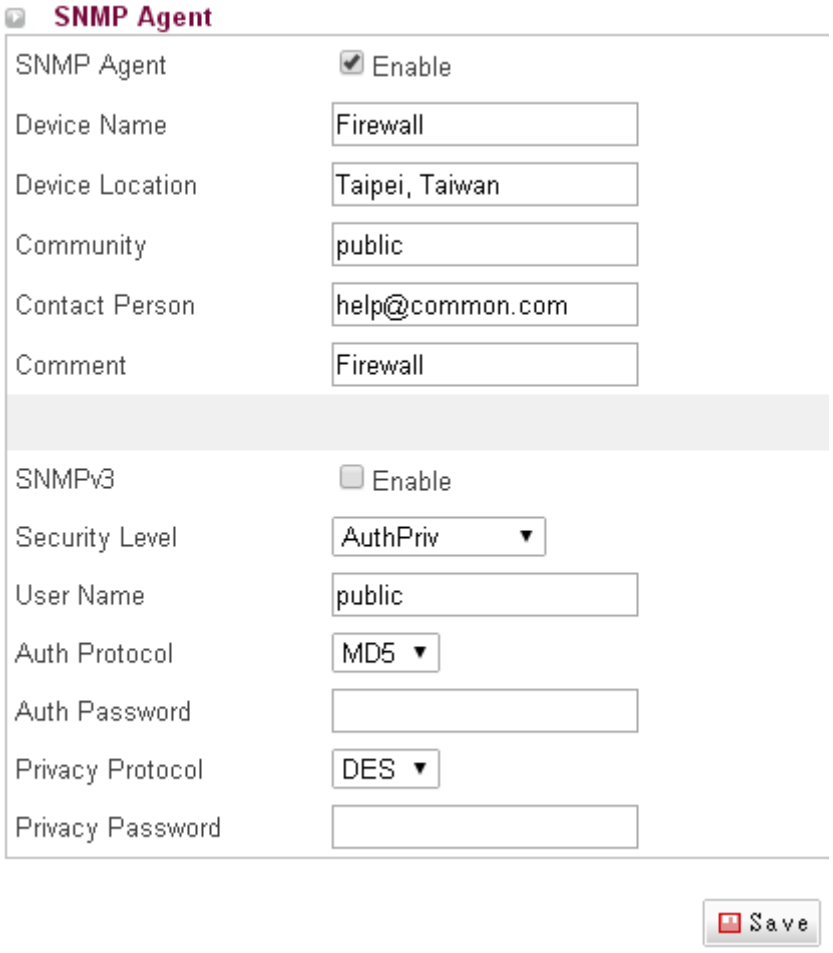


7.5 SNMP

SNMP (SNMP = Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Here, Axiomtek SNMP feature supports SNMPv3, and it primarily added security and remote configuration enhancements to SNMP. Besides, IT administrator can use SNMP plus MRTG to see more network status. In this section you can enable the following lists:

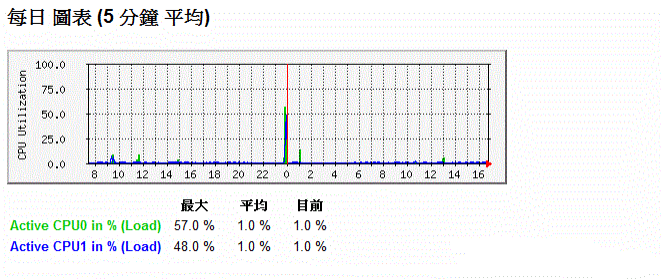
7.5.1 SNMP

Please select *Network Services* > *SNMP* > *SNMP*.

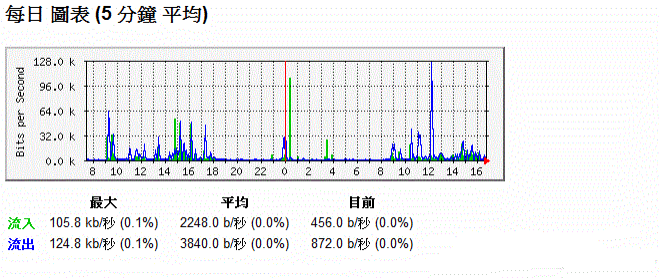


Here is some more network status:

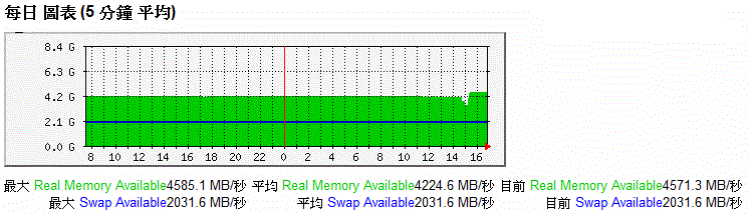
CPU usage:



Network traffic:



Memory loading:

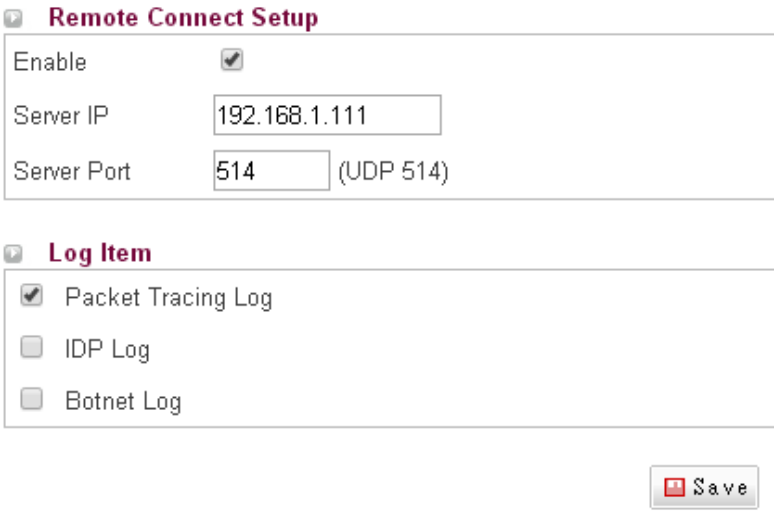

每日 圖表 (5 分鐘 平均)
8.4 G
6.3 G
4.2 G
2.1 G
0.0 G
8 10 12 14 16 18 20 22 0 2 4 6 8 10 12 14 16
最大 Real Memory Available4585.1 MB/秒 平均 Real Memory Available4224.6 MB/秒 目前 Real Memory Available4571.3 MB/秒
最大 Swap Available2031.6 MB/秒 平均 Swap Available2031.6 MB/秒 目前 Swap Available2031.6 MB/秒

7.6 Remote Syslog Server

IFW320 logs all its security functions so that you can analyze and do statistics. Also, there is a search function in all these log pages. Some abnormal behaviors of network can be located and then help you to fix. The log function is disabled by default.

7.6.1 Remote Connect Setup

Enabling IFW320 to send logs to the external syslog server, please select *Network Services* > *Remote Syslog Server* > *Remote Connect Setup*. Click "Enable" and enter the syslog server information.

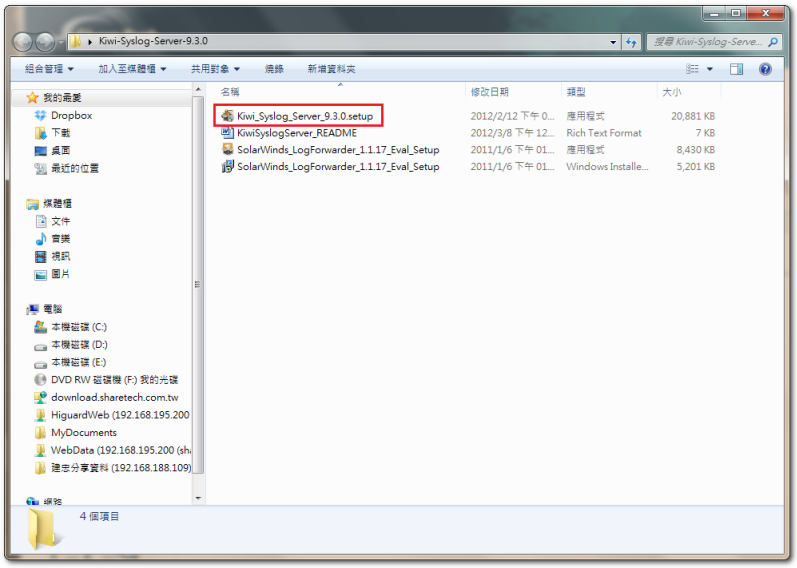


Example

Syslog is a service for remotely logging data. For example, it allows monitoring video with less network equipment. Here, I use Kiwi Syslog, please download the following link: http://www.kiwisyslog.com/downloads/registration.aspx?productType=ks&AppID=876&CampaignID=70150000000Es8J.

After that, please do:

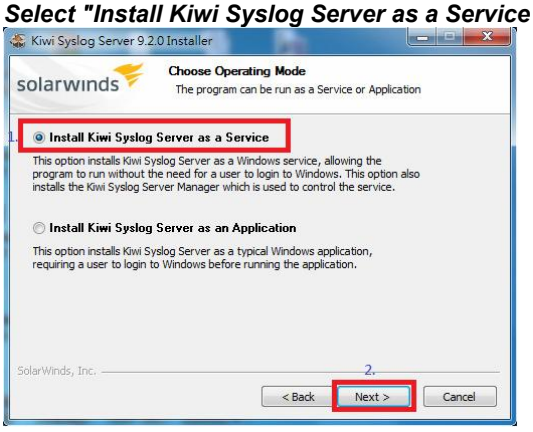
1. ***Click .exe file.***



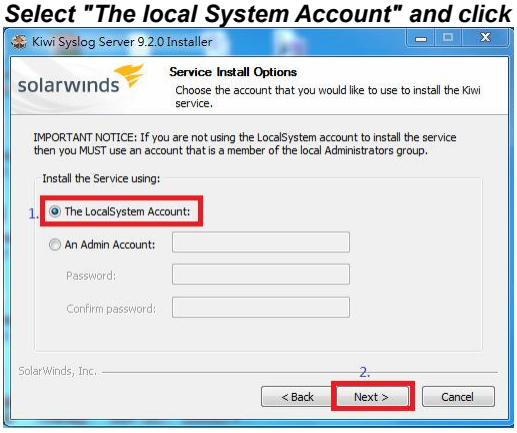
2. ***Select "I Agree".***

Kiwi Syslog Server 9.2.0 Installer
solarwinds
License Agreement
Please review the license terms before installing Kiwi Syslog Server 9.2.0 .
Press Page Down to see the rest of the agreement.
SOLARWINDS
END USER LICENSE AGREEMENT
IMPORTANT -- READ CAREFULLY BEFORE USING THIS SOFTWARE: THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND SOLARWINDS WORLDWIDE, LLC COVERING YOUR USE OF
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Kiwi Syslog Server 9.2.0 .
SolarWinds, Inc.
I Agree
Cancel

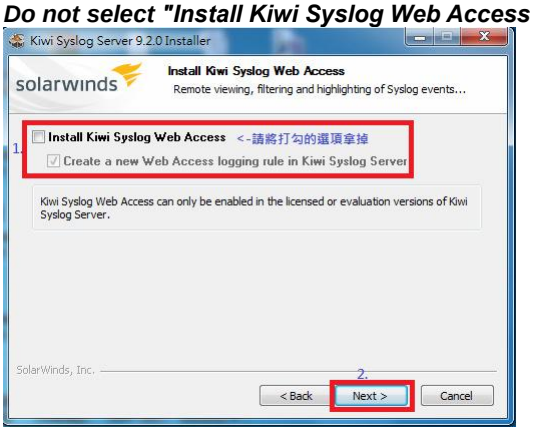
3. ***Select "Install Kiwi Syslog Server as a Service" and click on "Next".***


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Operating Mode
The program can be run as a Service or Application
1.
Install Kiwi Syslog Server as a Service
This option installs Kiwi Syslog Server as a Windows service, allowing the program to run without the need for a user to login to Windows. This option also installs the Kiwi Syslog Server Manager which is used to control the service.
Install Kiwi Syslog Server as an Application
This option installs Kiwi Syslog Server as a typical Windows application, requiring a user to login to Windows before running the application.
SolarWinds, Inc.
2.
< Back
Next >
Cancel

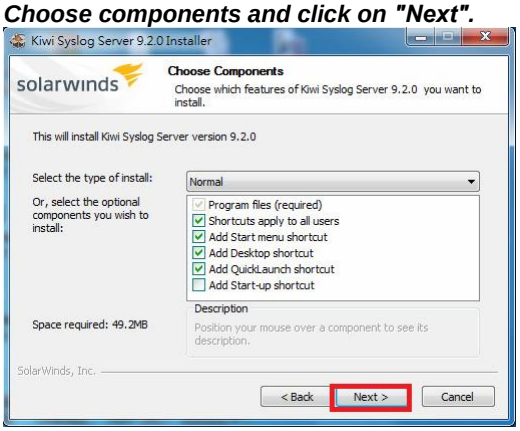
4. ***Select "The local System Account" and click on "Next".***


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Service Install Options
Choose the account that you would like to use to install the Kiwi service.
IMPORTANT NOTICE: If you are not using the LocalSystem account to install the service then you MUST use an account that is a member of the local Administrators group.
Install the Service using:
1.
The LocalSystem Account:
An Admin Account:
Password:
Confirm password:
SolarWinds, Inc.
2.
< Back
Next >
Cancel

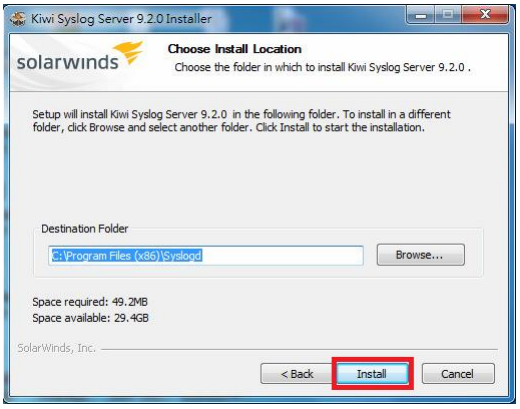
5. ***Do not select "Install Kiwi Syslog Web Access" and click on "Next".***


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Install Kiwi Syslog Web Access
Remote viewing, filtering and highlighting of Syslog events...
1.
Install Kiwi Syslog Web Access <-請將打勾的選項拿掉
Create a new Web Access logging rule in Kiwi Syslog Server
Kiwi Syslog Web Access can only be enabled in the licensed or evaluation versions of Kiwi Syslog Server.
SolarWinds, Inc.
2.
< Back
Next >
Cancel

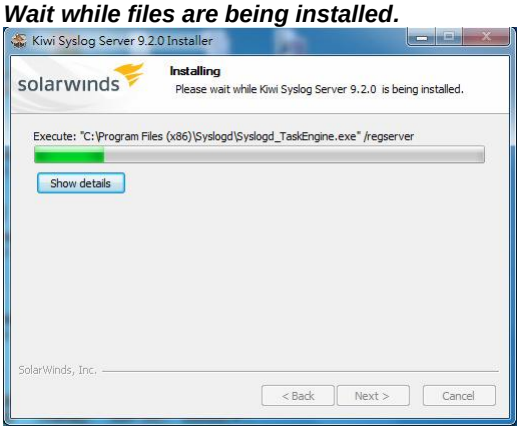
6. ***Choose components and click on "Next".***


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Components
Choose which features of Kiwi Syslog Server 9.2.0 you want to install.
This will install Kiwi Syslog Server version 9.2.0
Select the type of install:
Normal
Or, select the optional components you wish to install:
Program files (required)
Shortcuts apply to all users
Add Start menu shortcut
Add Desktop shortcut
Add QuickLaunch shortcut
Add Start-up shortcut
Description
Position your mouse over a component to see its description.
Space required: 49.2MB
SolarWinds, Inc.
< Back
Next >
Cancel

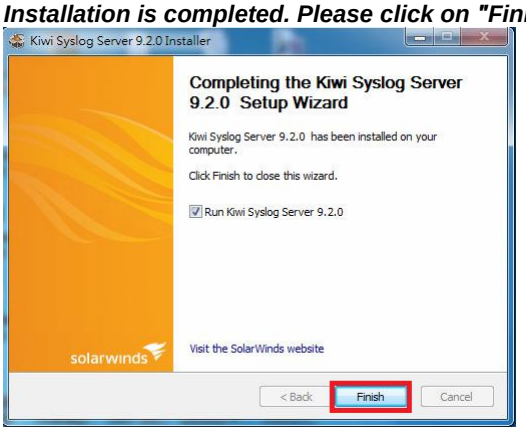
7. ***Choose destination folder and click on "Install".***


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Install Location
Choose the folder in which to install Kiwi Syslog Server 9.2.0 .
Setup will install Kiwi Syslog Server 9.2.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\Syslogd
Browse...
Space required: 49.2MB
Space available: 29.4GB
SolarWinds, Inc.
< Back
Install
Cancel

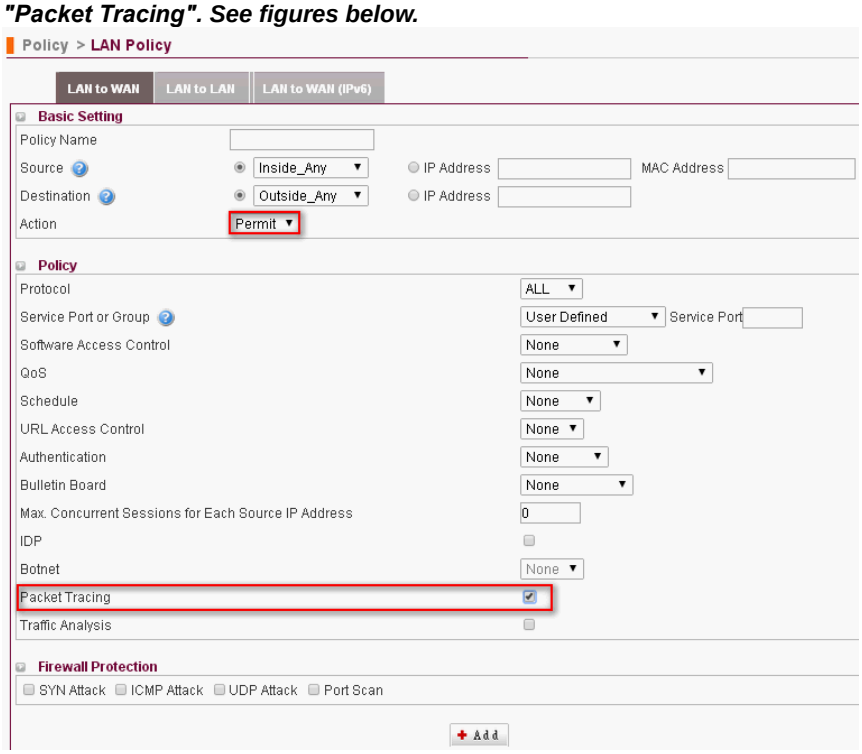
Wait while files are being installed.

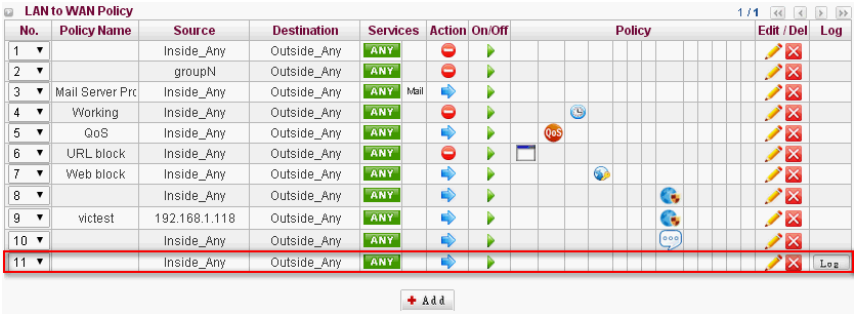


8. Installation is completed. Please click on "Finish".

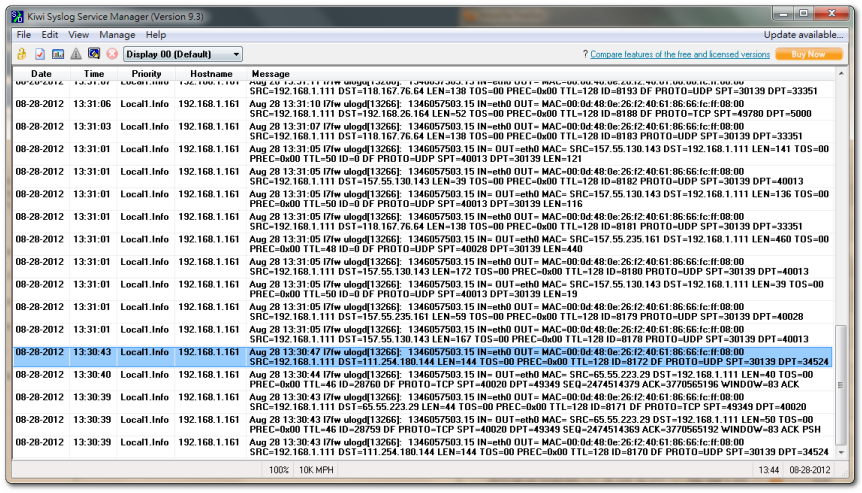

Kiwi Syslog Server 9.2.0 Installer
Completing the Kiwi Syslog Server 9.2.0 Setup Wizard
Kiwi Syslog Server 9.2.0 has been installed on your computer.
Click Finish to close this wizard.
Run Kiwi Syslog Server 9.2.0
solarwinds
Visit the SolarWinds website
< Back
Finish
Cancel

Please select Policy > LAN Policy > LAN to WAN, and must check on "Packet Tracing". See figures below.

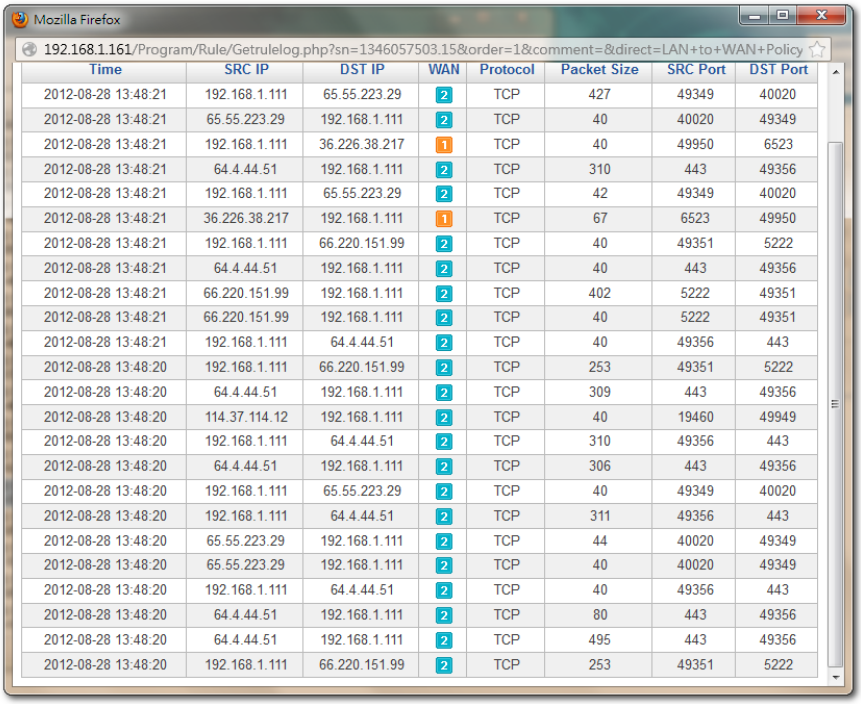




Then, you will see Syslog such as the following figure. It's similar like packet Tracing Log.



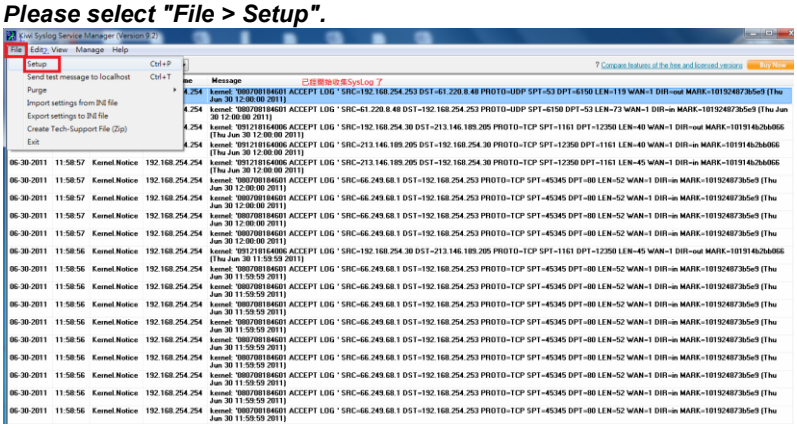
Please click on ***. Figure below shows packet Tracing Log.***



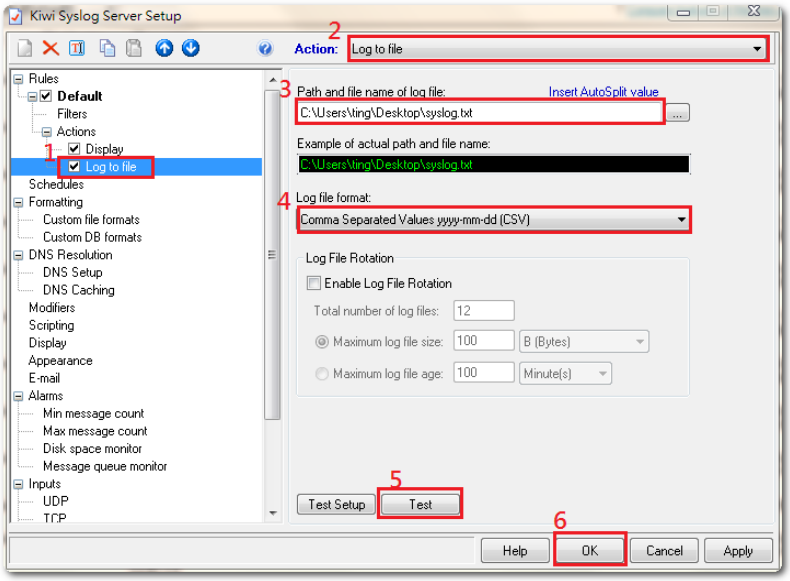
Caution

If you want to export syslog to .txt file, please follow steps below.

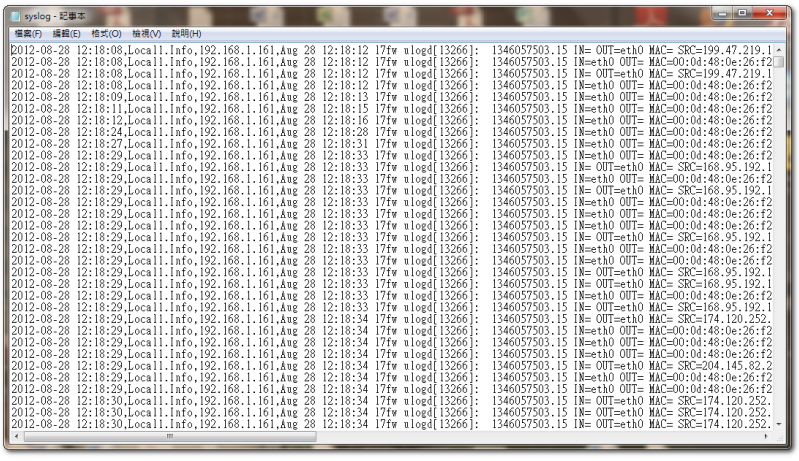
1. ***Please select "File > Setup".***



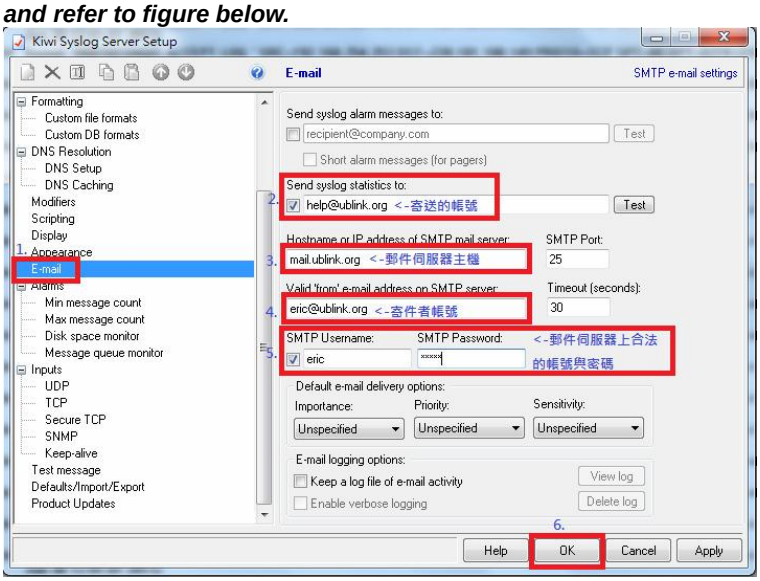
2. ***Please select "Log to file" and the rest are depend on your settings.***



3. ***Then, export syslog file is completing.***



4. ***Besides, users can also use mail Notification. Please select "E-mail" and refer to figure below.***



Chapter 8
Advanced Protection

An advanced protection of IFW320, CO-Defense SNMP, is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. When anomalous flow occurs, it will be blocked and the administrator will be notified and assisted to this abnormal situation. Defects can be known on which computer and which switch port at the earliest possible time which prevents business network from failure. IFW320 Co-Defense makes network management fairly easy because it does not need any change from network structure, habits of individual user, buying expensive Switch (with Layer 2), and extra detecting appliances.

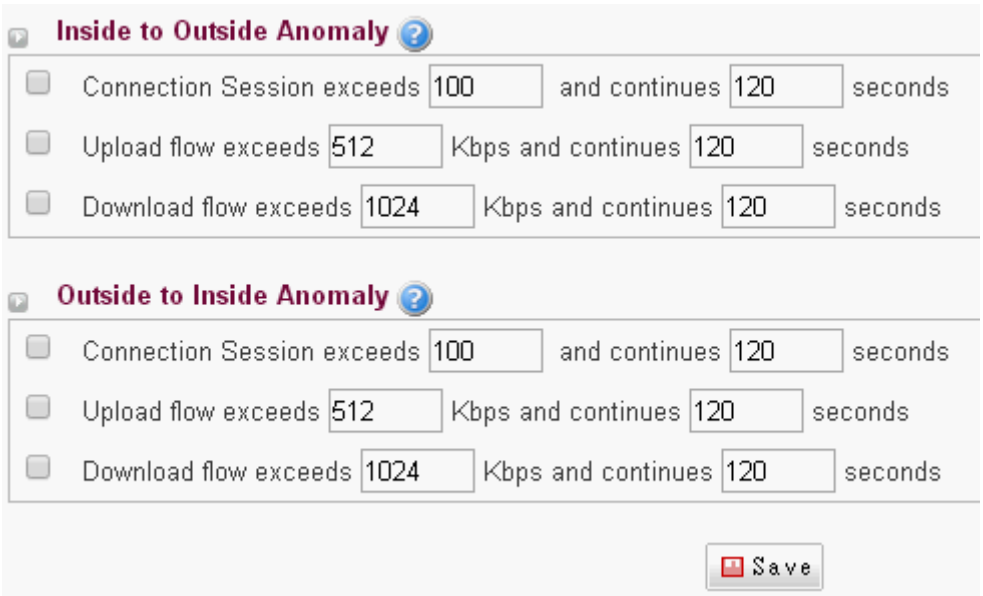
In the Advanced Protection chapter you can enable the following lists:

- Anomaly IP Analysis
- Switch Management
- Internal Protection

8.1 Anomaly IP Analysis

8.1.1 Log Anomaly

Select *Advanced Protection* > *Anomaly IP Analysis* > *Log Anomaly*.


Inside to Outside Anomaly
Connection Session exceeds 100 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Outside to Inside Anomaly
Connection Session exceeds 100 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Save

Outgoing Anomaly

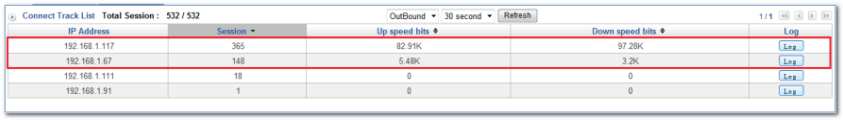
1. Session exceeds 100 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024 kbps and continues 120 seconds (default).

Incoming Anomaly

1. Session exceeds 100 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024 kbps and continues 120 seconds (default).

Example

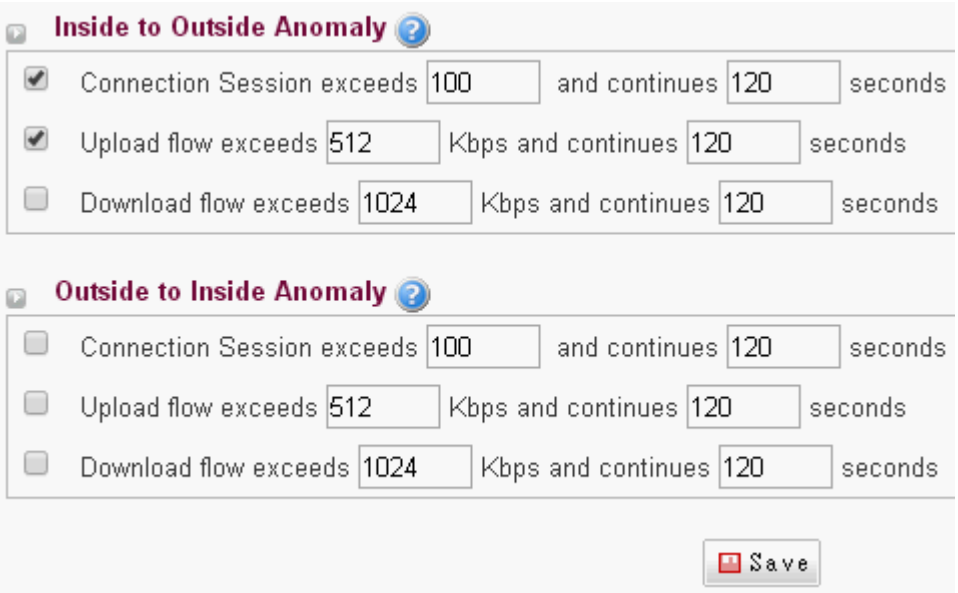
Enter "10" in outgoing anomaly and use "192.168.1.117" for testing this function. Let's see Status > Connection Status > Connect Track.



As we saw in the figure above, system should record "192.168.1.117" into log, so user can see logs in Advanced Protection > Anomaly IP Analysis > Anomaly Log.

8.1.2 Notify Anomaly

It accords with *Configuration > Administration > SMTP Server and Configuration > Notification > Notification.*


Inside to Outside Anomaly
Connection Session exceeds 100 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Outside to Inside Anomaly
Connection Session exceeds 100 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Save

Outgoing Anomaly

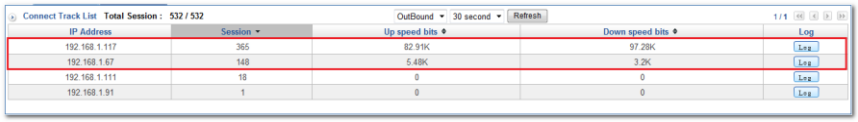
1. Session exceeds 100 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024 kbps and continues 120 seconds (default).

Incoming Anomaly

1. Session exceeds 100 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024 kbps and continues 120 seconds (default).

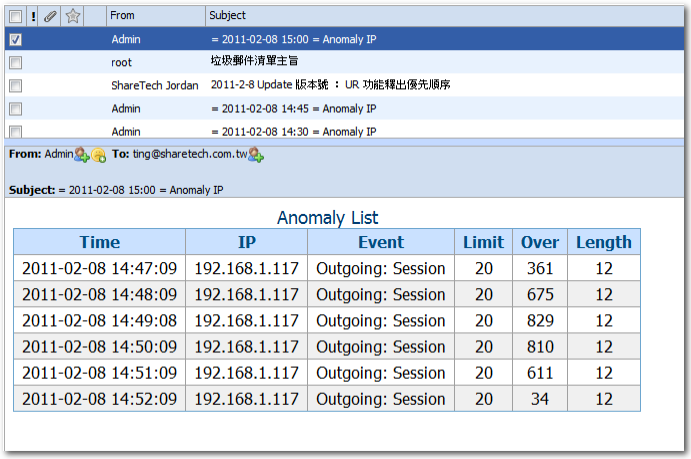
Example

Enter "20" in outgoing anomaly and use "192.168.1.117" for testing this function. Let's see Status > Connection Status > Connect Track.


Connect Track List Total Session : 532 / 532
OutBound 30 second Refresh
IP Address Session Up speed bits Down speed bits Log
192.168.1.117 365 82.91K 97.28K Log
192.168.1.67 148 6.48K 3.2K Log
192.168.1.111 18 0 0 Log
192.168.1.91 1 0 0 Log

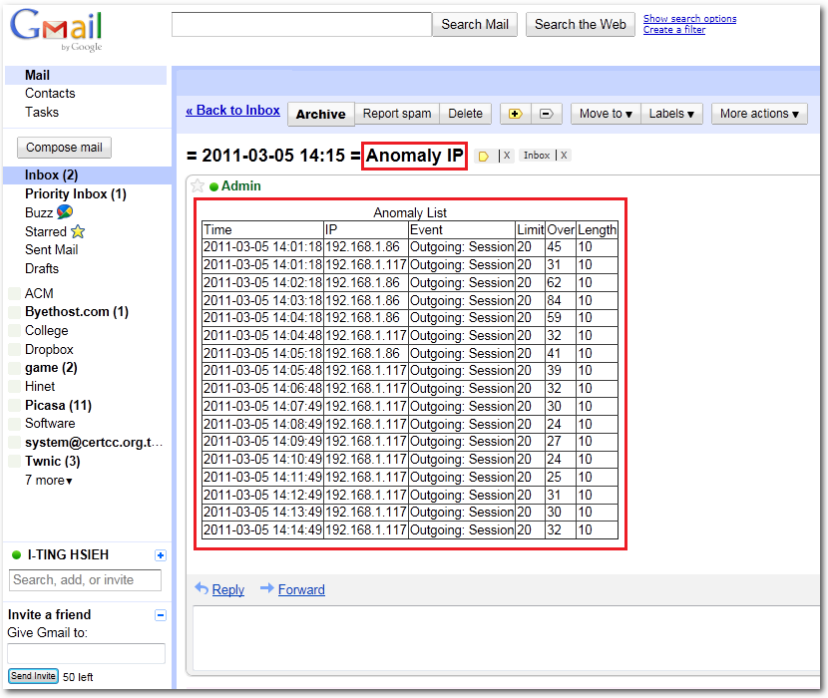
As we saw in the figure above, "192.168.1.117" should be recorded and system will mail logs to recipients. Then, user will receive notify logs such as figure below.

Notify email sample 1:


From Subject
Admin = 2011-02-08 15:00 = Anomaly IP
root 垃圾郵件清單主旨
ShareTech Jordan 2011-2-8 Update 版本號 ： UR 功能釋出優先順序
Admin = 2011-02-08 14:45 = Anomaly IP
Admin = 2011-02-08 14:30 = Anomaly IP
From: Admin To: ting@sharetech.com.tw
Subject: = 2011-02-08 15:00 = Anomaly IP
Anomaly List

Time	IP	Event	Limit	Over	Length
2011-02-08 14:47:09	192.168.1.117	Outgoing: Session	20	361	12
2011-02-08 14:48:09	192.168.1.117	Outgoing: Session	20	675	12
2011-02-08 14:49:08	192.168.1.117	Outgoing: Session	20	829	12
2011-02-08 14:50:09	192.168.1.117	Outgoing: Session	20	810	12
2011-02-08 14:51:09	192.168.1.117	Outgoing: Session	20	611	12
2011-02-08 14:52:09	192.168.1.117	Outgoing: Session	20	34	12

Notify email sample 2:



Time	IP	Event	Limit	Over	Length
2011-03-05 14:01:18	192.168.1.86	Outgoing: Session	20	45	10
2011-03-05 14:01:18	192.168.1.117	Outgoing: Session	20	31	10
2011-03-05 14:02:18	192.168.1.86	Outgoing: Session	20	62	10
2011-03-05 14:03:18	192.168.1.86	Outgoing: Session	20	84	10
2011-03-05 14:04:18	192.168.1.86	Outgoing: Session	20	59	10
2011-03-05 14:04:48	192.168.1.117	Outgoing: Session	20	32	10
2011-03-05 14:05:18	192.168.1.86	Outgoing: Session	20	41	10
2011-03-05 14:05:48	192.168.1.117	Outgoing: Session	20	39	10
2011-03-05 14:06:48	192.168.1.117	Outgoing: Session	20	32	10
2011-03-05 14:07:49	192.168.1.117	Outgoing: Session	20	30	10
2011-03-05 14:08:49	192.168.1.117	Outgoing: Session	20	24	10
2011-03-05 14:09:49	192.168.1.117	Outgoing: Session	20	27	10
2011-03-05 14:10:49	192.168.1.117	Outgoing: Session	20	24	10
2011-03-05 14:11:49	192.168.1.117	Outgoing: Session	20	25	10
2011-03-05 14:12:49	192.168.1.117	Outgoing: Session	20	31	10
2011-03-05 14:13:49	192.168.1.117	Outgoing: Session	20	30	10
2011-03-05 14:14:49	192.168.1.117	Outgoing: Session	20	32	10

8.1.3 Block Anomaly

Outgoing Anomaly

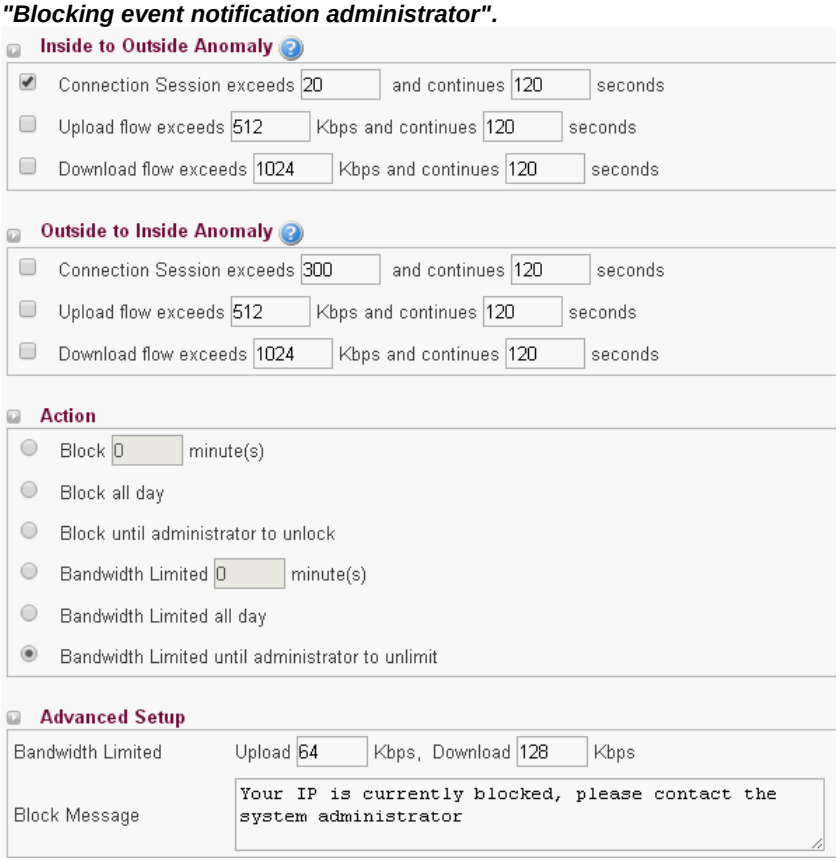
1. Session exceeds 100 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024kbps and continues 120 seconds (default).

Incoming Anomaly

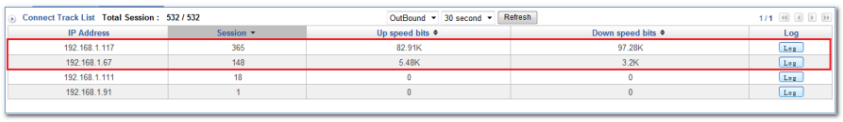
1. Session exceeds 300 and continues 120 seconds (default).
2. Upload flow exceeds 512 kbps and continues 120 seconds (default).
3. Download flow exceeds 1024 kbps and continues 120 seconds (default).

Example

Enter "20" in outgoing anomaly and use "192.168.1.117" for testing this function. In addition, select "Block until administrator to unlock" and "Blocking event notification administrator".


Inside to Outside Anomaly
Connection Session exceeds 20 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Outside to Inside Anomaly
Connection Session exceeds 300 and continues 120 seconds
Upload flow exceeds 512 Kbps and continues 120 seconds
Download flow exceeds 1024 Kbps and continues 120 seconds
Action
Block 0 minute(s)
Block all day
Block until administrator to unlock
Bandwidth Limited 0 minute(s)
Bandwidth Limited all day
Bandwidth Limited until administrator to unlimit
Advanced Setup
Bandwidth Limited
Upload 64 Kbps, Download 128 Kbps
Block Message
Your IP is currently blocked, please contact the system administrator

Let's see Status > Connection Status > Connect Track.

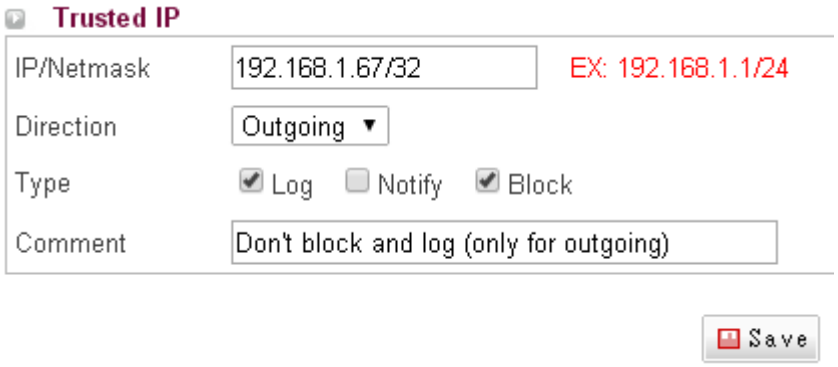


As we saw in the figure above, "192.168.1.117" should be blocked, so user can see block lists in Advanced Protection > Anomaly IP Analysis > Block List.

8.1.4 Trusted IP

If user has some IP addresses which do not want to be restricted by this function, user could enter the IP ranges. After that those IPs you entered would not be detected by anomaly analysis.

IP exception setting:

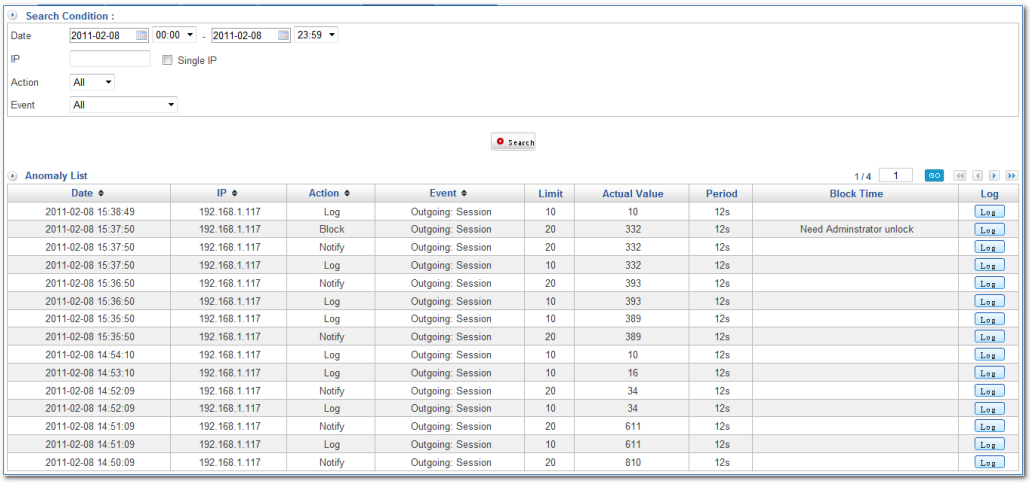


Setting IP exception completed:

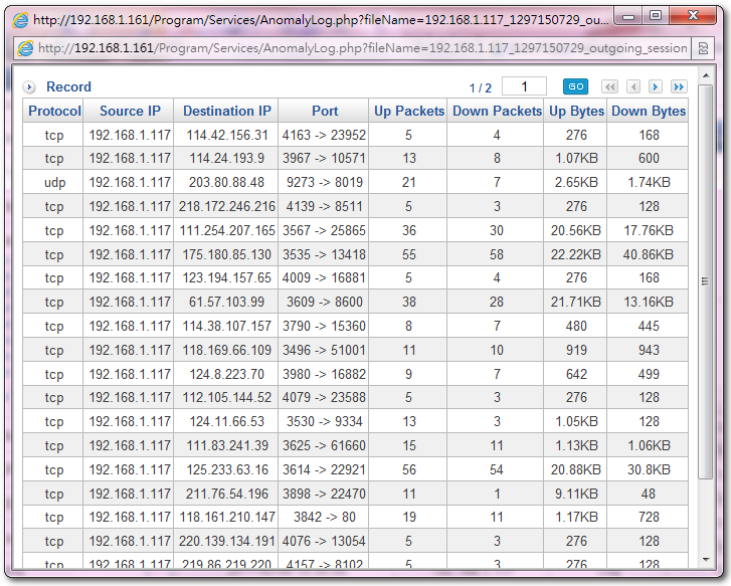
8.1.5 Anomaly Log

You can find anomaly log at *Advanced Protection > Anomaly IP Analysis > Anomaly Log.*

Anomaly search:



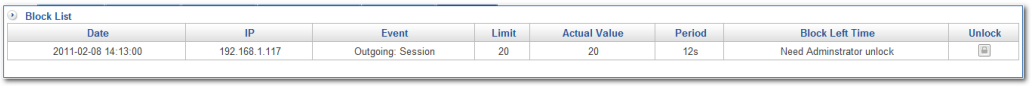
Anomaly log:



Protocol	Source IP	Destination IP	Port	Up Packets	Down Packets	Up Bytes	Down Bytes
tcp	192.168.1.117	114.42.156.31	4163 -> 23952	5	4	276	168
tcp	192.168.1.117	114.24.193.9	3967 -> 10571	13	8	1.07KB	600
udp	192.168.1.117	203.80.88.48	9273 -> 8019	21	7	2.65KB	1.74KB
tcp	192.168.1.117	218.172.246.216	4139 -> 8511	5	3	276	128
tcp	192.168.1.117	111.254.207.165	3567 -> 25865	36	30	20.56KB	17.76KB
tcp	192.168.1.117	175.180.85.130	3535 -> 13418	55	58	22.22KB	40.86KB
tcp	192.168.1.117	123.194.157.65	4009 -> 16881	5	4	276	168
tcp	192.168.1.117	61.57.103.99	3609 -> 8600	38	28	21.71KB	13.16KB
tcp	192.168.1.117	114.38.107.157	3790 -> 15360	8	7	480	445
tcp	192.168.1.117	118.169.66.109	3496 -> 51001	11	10	919	943
tcp	192.168.1.117	124.8.223.70	3980 -> 16882	9	7	642	499
tcp	192.168.1.117	112.105.144.52	4079 -> 23588	5	3	276	128
tcp	192.168.1.117	124.11.66.53	3530 -> 9334	13	3	1.05KB	128
tcp	192.168.1.117	111.83.241.39	3625 -> 61660	15	11	1.13KB	1.06KB
tcp	192.168.1.117	125.233.63.16	3614 -> 22921	56	54	20.88KB	30.8KB
tcp	192.168.1.117	211.76.54.196	3898 -> 22470	11	1	9.11KB	48
tcp	192.168.1.117	118.161.210.147	3842 -> 80	19	11	1.17KB	728
tcp	192.168.1.117	220.139.134.191	4076 -> 13054	5	3	276	128
tcp	192.168.1.117	219.86.219.220	4157 -> 8102	5	3	276	128

8.1.6 Block List

It accords with *Advanced Protection* > *Anomaly IP Analysis* > *Block Anomaly*. If user have selected "Block until administrator to unlock" in block setting, don't forget to click on to unlock that IP.



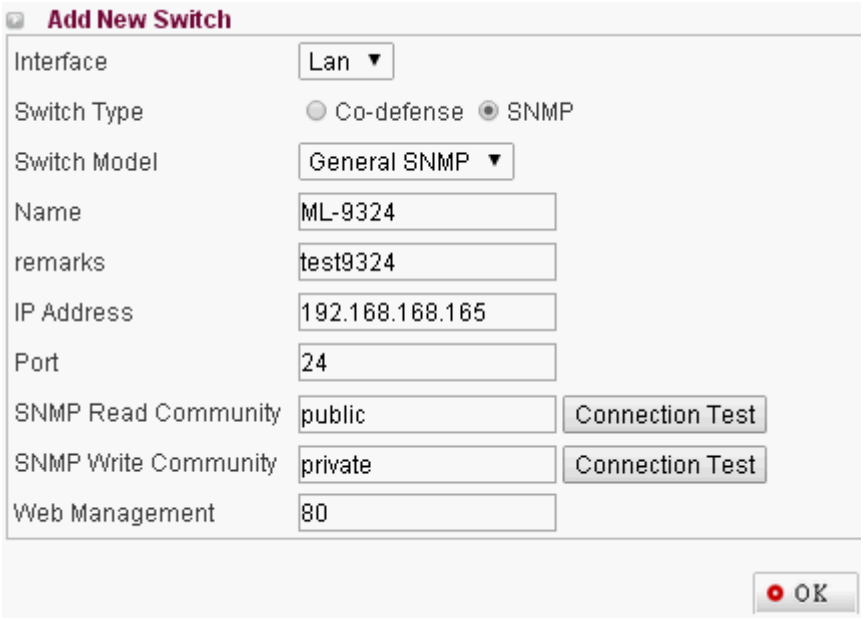
Date	IP	Event	Limit	Actual Value	Period	Block Left Time	Unlock
2011-02-08 14:13:00	192.168.1.117	Outgoing: Session	20	20	12s	Need Adminstrator unlock	

8.2 Switch Management

The network switch plays an integral part in most modern Ethernet local area networks (LANs). Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as a residential gateway to access small office/home broadband services such as DSL or cable Internet. In most of these cases, the end-user device contains a router and components that interface to the particular physical broadband technology. User devices may also include a telephone interface for VoIP.

8.2.1 Switch Setup

A network switch or switching hub is a computer networking device that connects network segments. Select *Advanced Protection* > *Switch Management* > *Switch Setup*. Click on to create a new switch.



Interface
Choose which IFW320 interface your switch is connecting to.

Switch Type
Choose what kinds of function you need.

1. Co-Defense: Four models below are supported.
   a. AG-2824T
   b. ML-9324
   c. ML-9308
   d. 3Com-4210
2. SNMP Switch: Select what kind of switch you used.
   a. General SNMP Switch
   b. Switch ML-9324

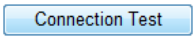
Switch Model
It depends on what you choose on switch type.

Name
Enter switch model name.

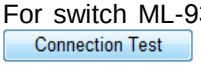
Remarks
Enter any words for recognition.

IP Address
Enter switch IP address.

Number of Port
Total number of switch port.

SNMP Read Community
For switch ML-9324, default read community is "public." Administrator could click on 

to check connection.

SNMP Write Community
For switch ML-9324, default write community is "private." Administrator could click on 

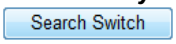
to check connection.

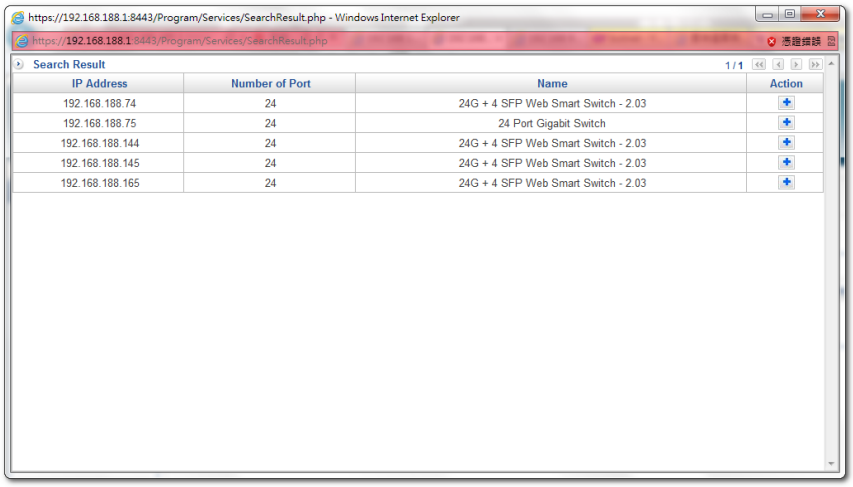
Web Management
Enter switch web management port. Default port is 80.

Let's click on to create a new switch connection.

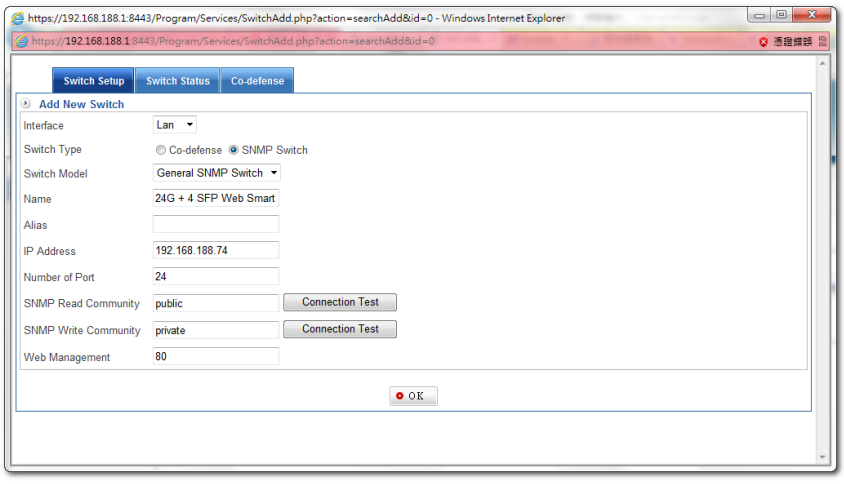
After click on , you will see switch list. Figure below shows SNMP Switch is created successfully.

Note

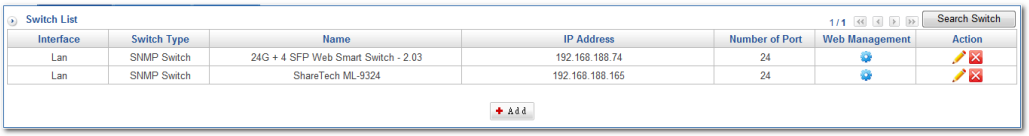
If IT administrator doesn't know the switch IP or doesn't know how many switches are under IFW320, IT administrator could click on  ***to scan (search) for switches. The Search Result is shown in figure below.***



Click on ***to add switch and click on*** ***to create a new one.***



Setting switch completed. In addition, click on Add to create a new sub-content, to modify contents, or to cancel list.



8.3 Internal Protection

It has been the most difficult for firewall appliance to detect broadcast package sent out on the local network such as ARP spoofing and private DHCP server because of congenital detects of communication protocols. Axiomtek IFW320 can effectively detect who is the man-in-the-middle attack. With a Co-defense switch, physical IP destination can be marked.

8.3.1 Spoofing Setup

Select *Advanced Protection* > *Internal Protection* > *Spoofing Setup*.

Detection Interface
LAN
DMZ
ARP Spoofing Alert Value
Each source ip address exceeds 100 ARP packets/s . (Minimum value is 50)
Automatically Block by Switch
Collision Detection : IP
IP Address Collision Detection
Automatically Block by Switch
Collision Detection : MAC
MAC Address Collision Detection 3 times / hour. Block it by switch
Automatically Block by Switch
Router mac
True Address
Co-defense
Linked abnormal IP block list Port Close
Linked Botnet Port Close 20 times / minute . Block it by switch
Notify Item
Linked abnormal IP block
Botnet Port blocking linked
Arp Protection
IP collision
MAC collision

Detection Interface
Click to choose an interface(s) applying security mechanisms. There are 2 options here-LAN and DMZ.

ARP Spoofing Alert Value
ARP Protection. Larger value means lower sensitivity.

Collision Detection : IP
Enable auto block to violated IP addresses. If it is enabled, the access port which has the violated IP will be shut down.

Collision Detection : MAC
Enable auto block to violated MAC addresses. Default is to detect collision 3 times per hour. If forgery is discovered, it will be blocked instantly. Administrators can also setup trusted MAC list.

Linked abnormal IP block list Port Close
The switch port will shut down once IP address exceeds the set values.

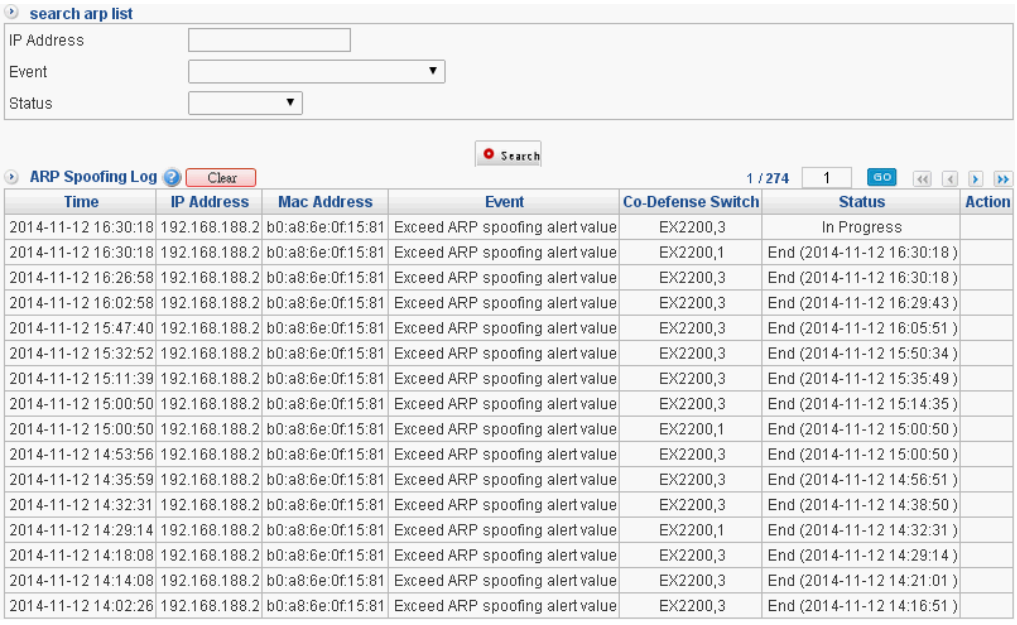
Linked Botnet Port Close
If the BotNet attacks exceed the set value (times/minute), protection will be enabled. And the switch port will shut down once IP address exceeds the set values.

Notify Item
When events mentioned above occur, an email will send out to notify the administrator. Notify items included Linked abnormal IP block, BotNet Port blocking linked, ARP Protection, IP collision and MAC collision.

8.3.2 ARP Spoofing Log

ARP Spoofing Log contains time, IP address, MAC address, Event, Co-Defense Switch, Status, and Action. It splits the attackers and the victims allowing administrators to trouble shoot with efficient.

Select Advanced *Protection* > *Internal Protection* > *ARP Spoofing Log*.



Time	IP Address	Mac Address	Event	Co-Defense Switch	Status	Action
2014-11-12 16:30:18	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	In Progress	
2014-11-12 16:30:18	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,1	End (2014-11-12 16:30:18)	
2014-11-12 16:26:58	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 16:30:18)	
2014-11-12 16:02:58	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 16:29:43)	
2014-11-12 15:47:40	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 16:05:51)	
2014-11-12 15:32:52	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 15:50:34)	
2014-11-12 15:11:39	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 15:35:49)	
2014-11-12 15:00:50	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 15:14:35)	
2014-11-12 15:00:50	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,1	End (2014-11-12 15:00:50)	
2014-11-12 14:53:56	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 15:00:50)	
2014-11-12 14:35:59	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 14:56:51)	
2014-11-12 14:32:31	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 14:38:50)	
2014-11-12 14:29:14	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,1	End (2014-11-12 14:32:31)	
2014-11-12 14:18:08	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 14:29:14)	
2014-11-12 14:14:08	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 14:21:01)	
2014-11-12 14:02:26	192.168.188.2	b0:a8:6e:0f:15:81	Exceed ARP spoofing alert value	EX2200,3	End (2014-11-12 14:16:51)	

IP Address
This IP address is found in which switch port.

Event
If co-defense is enabled, administrators can look up the problem by quickly searching exceeding values and victim conditions.

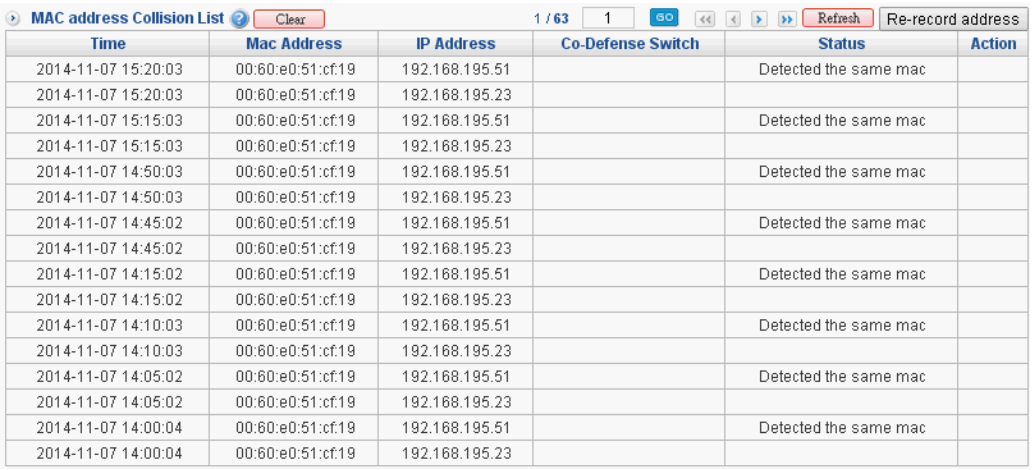
Status
Attacking is carrying on or stopped.

Search
Search for functions and log according to certain specific conditions.

8.3.3 MAC Collision Log

MAC Collision Log displays any forged MAC address within the internal network allowing administrators to trouble shoot efficiently.

Select *Advanced Protection* > *Internal Protection* > *MAC Collision Log*.


MAC address Collision List Clear 1 / 63 1 GO Refresh Re-record address

Time	Mac Address	IP Address	Co-Defense Switch	Status	Action
2014-11-07 15:20:03	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 15:20:03	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 15:15:03	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 15:15:03	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:50:03	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:50:03	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:45:02	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:45:02	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:15:02	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:15:02	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:10:03	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:10:03	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:05:02	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:05:02	00:60:e0:51:cf:19	192.168.195.23			
2014-11-07 14:00:04	00:60:e0:51:cf:19	192.168.195.51		Detected the same mac	
2014-11-07 14:00:04	00:60:e0:51:cf:19	192.168.195.23			

MAC Address
Find out which MAC address is being forged.

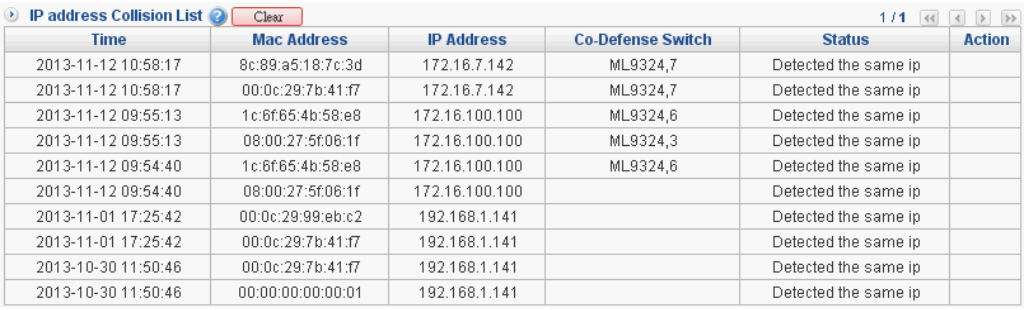
IP Address
Which IP address is the forged MAC address.

Co-Defense Switch
Find out which switch is connected to.

8.3.4 IP Collision Log

IP Collision Log displays any forged IP address within the internal network allowing administrators to trouble shoot efficiently.

Select *Advanced Protection* > *Internal Protection* > *IP Collision Log*.


IP address Collision List Clear 1 / 1

Time	Mac Address	IP Address	Co-Defense Switch	Status	Action
2013-11-12 10:58:17	8c:89:a5:18:7c:3d	172.16.7.142	ML9324,7	Detected the same ip	
2013-11-12 10:58:17	00:0c:29:7b:41:f7	172.16.7.142	ML9324,7	Detected the same ip	
2013-11-12 09:55:13	1c:6f:65:4b:58:e8	172.16.100.100	ML9324,6	Detected the same ip	
2013-11-12 09:55:13	08:00:27:5f:06:1f	172.16.100.100	ML9324,3	Detected the same ip	
2013-11-12 09:54:40	1c:6f:65:4b:58:e8	172.16.100.100	ML9324,6	Detected the same ip	
2013-11-12 09:54:40	08:00:27:5f:06:1f	172.16.100.100		Detected the same ip	
2013-11-01 17:25:42	00:0c:29:99:eb:c2	192.168.1.141		Detected the same ip	
2013-11-01 17:25:42	00:0c:29:7b:41:f7	192.168.1.141		Detected the same ip	
2013-10-30 11:50:46	00:0c:29:7b:41:f7	192.168.1.141		Detected the same ip	
2013-10-30 11:50:46	00:00:00:00:00:01	192.168.1.141		Detected the same ip	

MAC Address
Which MAC address is being forged.

IP Address
Which MAC address is the forged IP address.

Status
Which one is the problematic IP address.

8.3.5 Lock Status

When source IP address sends traffic that exceeds the set value, IFW320 will list out the suspicious IPs and block them. Lock Status contains ARP, MAC, IP, BotNet, and Anomaly IP.

Select *Advanced Protection* > *Internal Protection* > *Lock Status*.

Chapter 9
IDP & BotNet

Traditional firewall can inspect Layer 2 to Layer 4 of OSI model, such as Source IP Address, Destination IP Address, Source Port Number, Destination Port Number, and Flag Fields. However, traditional defense system cannot protect industry's network from evolving threats and virus anymore.

Axiomtek IFW320's built-in IDP (IDP = Intrusion Detection and Prevention, IDS + IPS) can inspect the packets from OSI layer 4 (transport layer) to OSI layer 7 (application layer) by using Deep Packet Inspection (DPI), and block concealed malicious code, such as worms and buffer overflow attacks. As soon as an attack is suspected, IFW320 will immediately notify the IT administrator. Moreover, an extensive range of reports is available for the IT administrator to analyze.

Integrated IDP system with attack-signature database protects industries from network threats, such as Trojan horse, virus, worms, buffer overflow etc. Take worm as an example, to protect attack from worm, the only thing for firewall to do is to close ports. As for the file-based virus, it is outside the scope of firewall protection. Axiomtek IFW320's built-in IDP with huge database can inspect all the packets from WEB, P2P, IM, NetBIOS etc.

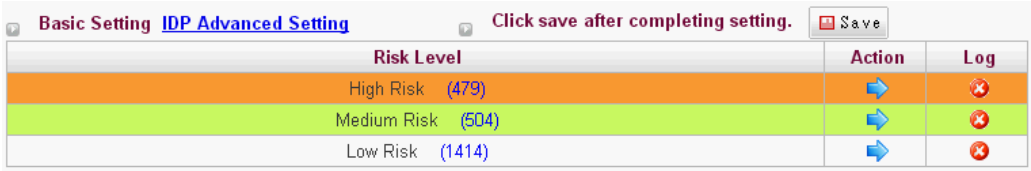
- IDP Setting
- IDP Log
- BotNet Setting
- BotNet Log

9.1 IDP Setting

In order to protect your network from various security threats, the device produces timely alerts and blocking mechanisms based upon anomaly flows and the inspection of packet contents. Thus, it ensures that the network's performance remains efficient and uninhibited. This section deals with the configuration settings of IDP. IFW320 includes the well-known IDS (IDS = Intrusion Detection System) and IPS (Intrusion Prevention System) system Snort. It is directly built into the IP-firewall (Snort inline). At this time no rules can be added through the web interface, hence Snort is usable only for advanced users that can load their own rules through the command line.

9.1.1 Basic Setting

Select *IDP & BotNet* > *IDP Setting* > *Basic Setting*.



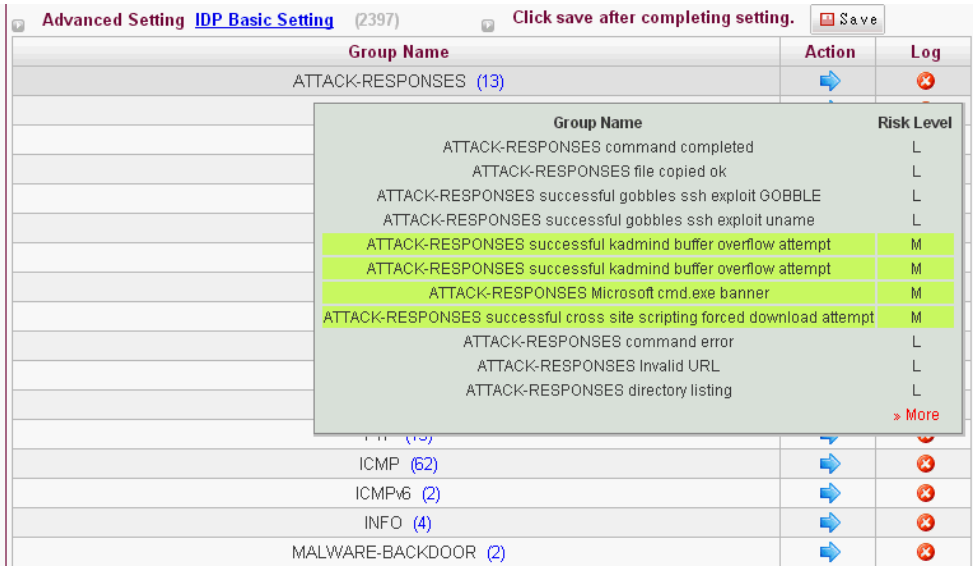
Risk Level
The risk level

Action
Click on Action button.
1. : On.
2. : Off.

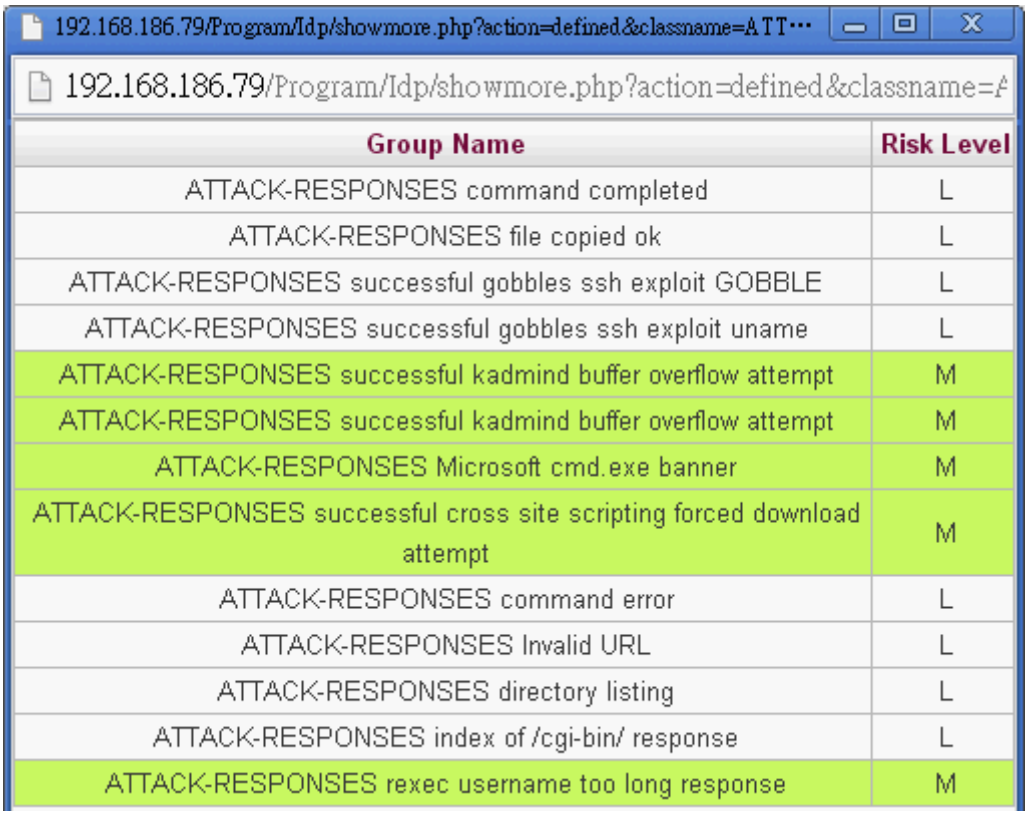
Log
Click on Log button.
1. : On.
2. : Off.

Save
After completing this model setting, please click on Save.

Click on IDP Advanced Settings link
And you will see a screen as shown is figure below. On the other hand, click on IDP Basic Setting to get back to previous step. After setting your IDP function, do not forget to click on Save. In addition, click rectangular form if you want to see class name list.



Click on "» More" to see more detail of risk group name.



Group Name	Risk Level
ATTACK-RESPONSES command completed	L
ATTACK-RESPONSES file copied ok	L
ATTACK-RESPONSES successful gobbles ssh exploit GOBBLE	L
ATTACK-RESPONSES successful gobbles ssh exploit uname	L
ATTACK-RESPONSES successful kadmind buffer overflow attempt	M
ATTACK-RESPONSES successful kadmind buffer overflow attempt	M
ATTACK-RESPONSES Microsoft cmd.exe banner	M
ATTACK-RESPONSES successful cross site scripting forced download attempt	M
ATTACK-RESPONSES command error	L
ATTACK-RESPONSES Invalid URL	L
ATTACK-RESPONSES directory listing	L
ATTACK-RESPONSES index of /cgi-bin/ response	L
ATTACK-RESPONSES rexec username too long response	M

9.2 IDP Log

9.2.1 IDP Log

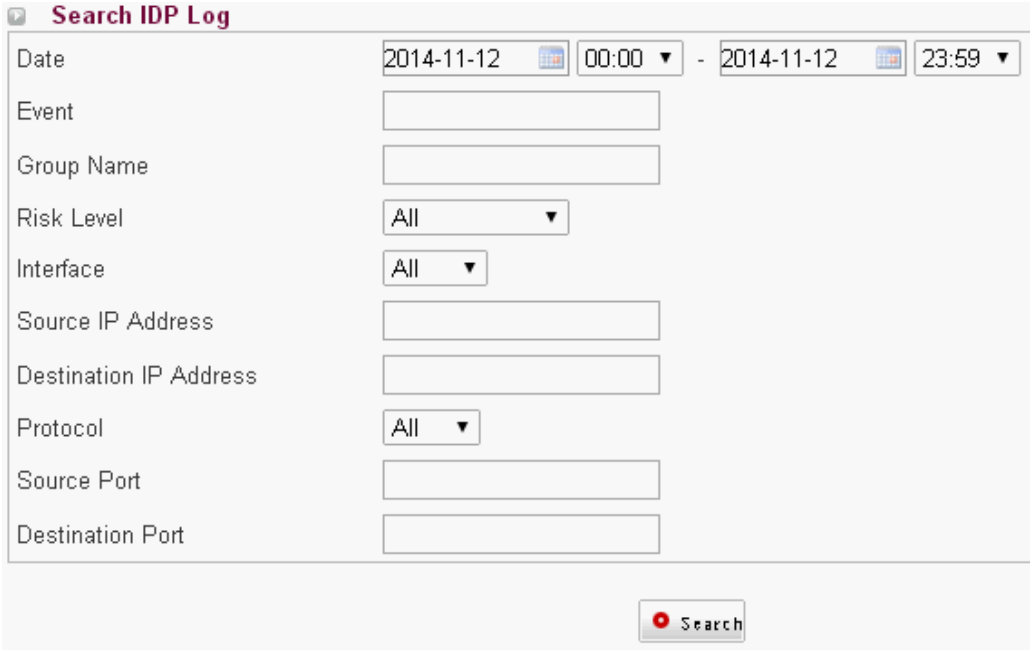
Select *IDP & BotNet > IDP Log > IDP Log*.

IDP Log List
IT administrators can see IDP log here.

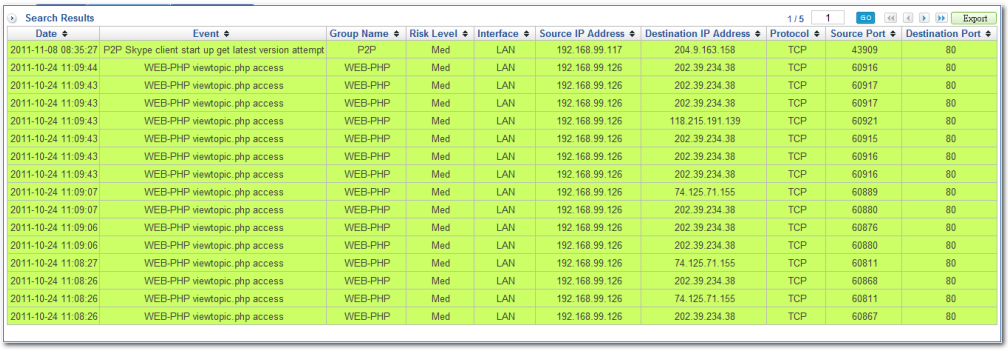
9.2.2 IDP Log Search

Select or type information you want to search (see figure below), and click on

.



After clicking on Search, you will see Logs Search Result as shown in example below.

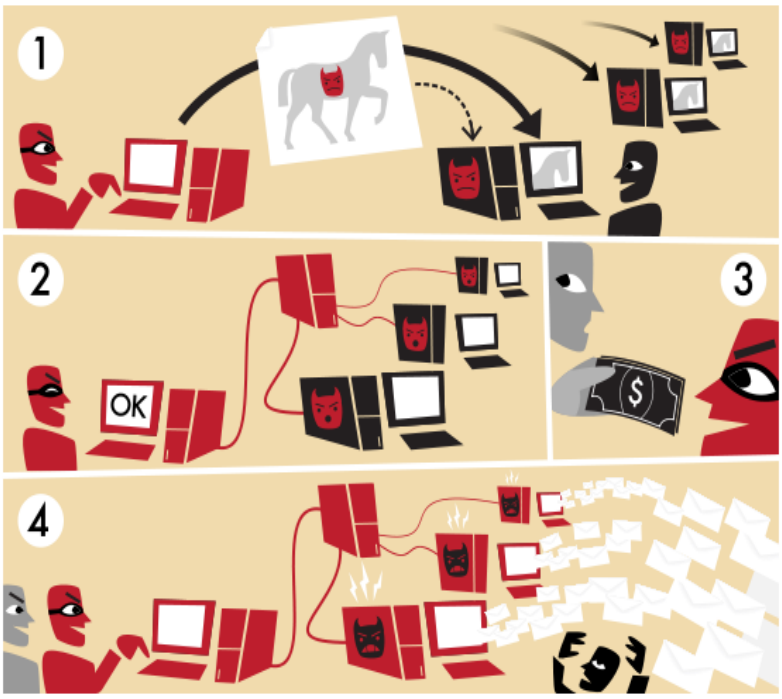


Date	Event	Group Name	Risk Level	Interface	Source IP Address	Destination IP Address	Protocol	Source Port	Destination Port
2011-11-08 08:35:27	P2P Skype client start up get latest version attempt	P2P	Med	LAN	192.168.99.117	204.9.163.158	TCP	43909	80
2011-10-24 11:09:44	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60917	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60917	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	118.215.191.139	TCP	60921	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60915	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:07	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60889	80
2011-10-24 11:09:07	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60880	80
2011-10-24 11:09:06	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60876	80
2011-10-24 11:09:06	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60880	80
2011-10-24 11:08:27	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60811	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60868	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60811	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60867	80

9.3 BotNet Setting

Traditional built-in UTM firewalls and safeguards can no longer be an effective defense against new virus attack, “bot” (also known as a zombie). Criminals typically use bots to infect large numbers of computers and these form a network, called a “botnet”.

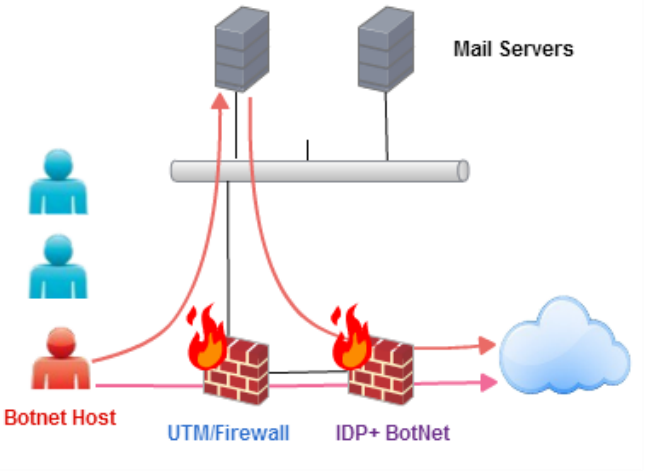
How do you know you have an infected computer?
A bot is often created through an Internet port which has been left open without scheduled update. A small Trojan horse program can be left for future activation. Visiting malicious websites, exchanging multi-media files or transferring through USB drivers can make you your computer infected. When a command is released from the zombie army "controller", your computer performs automated tasks over the Internet, without you knowing it. Being a vulnerable server to the swarm, your computer will send spam distribution to many computers.



How BotNet works. Source: http://en.wikipedia.org/wiki/Botnet

Why traditional Firewall and IDP do not work?
Attacks had always been assumed to come from external network; therefore, security suits such as firewall, IDP, and anti-virus with constant and timely updates were built for different levels of protection.

IDP (Intrusion Detection and Prevention) is primarily focused on identifying possible incidents, logging information about them, and reporting attempts. Generally, it is built outside a firewall to detect Trojan signature efficiently.

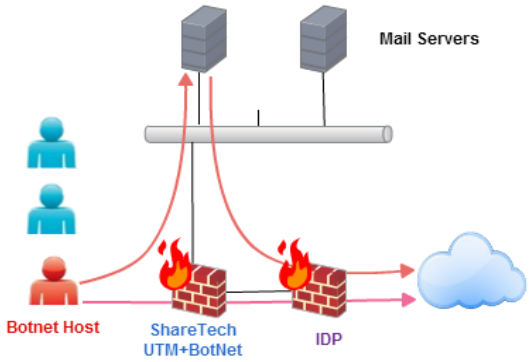


Traditional IDP cannot find BotNet

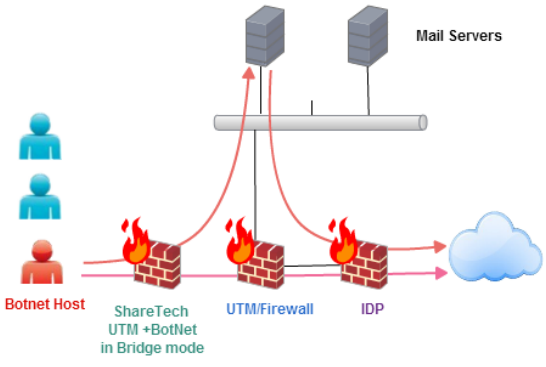
IDP has signature to detect BotNet and points out problems within mail server, internal server, or package from external IP. In the meanwhile, administrators thought appliances were infected and was ready to delete virus and reboot the system; however, problems cannot be solved. Traditional network security appliances were made under assumption that "The internal network is safe." which now becomes the chief defect.

Solution

Axiomtek UTM integrated with BotNet together with in-built NAT; it can explicitly point out the real attack running hidden and suspense malicious software spreading in the internal network.



UTM integrated with BotNet



Integrated with original UTM/Firewall

If a firewall has been built in the network environment, the figure on the left is for your reference. Please enable Axiomtek Bridge mode. All packets going through original UTM or firewall will be detected and the problematic computer will be found as well.

9.3.1 Operation Mode

Select *IDP & BotNet > BotNet Setting > Operation Mode*.

Before importing zombie blocking mechanism, enable “Sniffer” mode and all packets will be led to engine. After analyzing log for several days, we can know we are being infected or not.

In “Sniffer” mode, malicious packets cannot be blocked. If direct blocking is necessary, please enable “Inline” mode applied with policy and “Botnet Filter Setting.”

9.3.2 BotNet Filter Setting

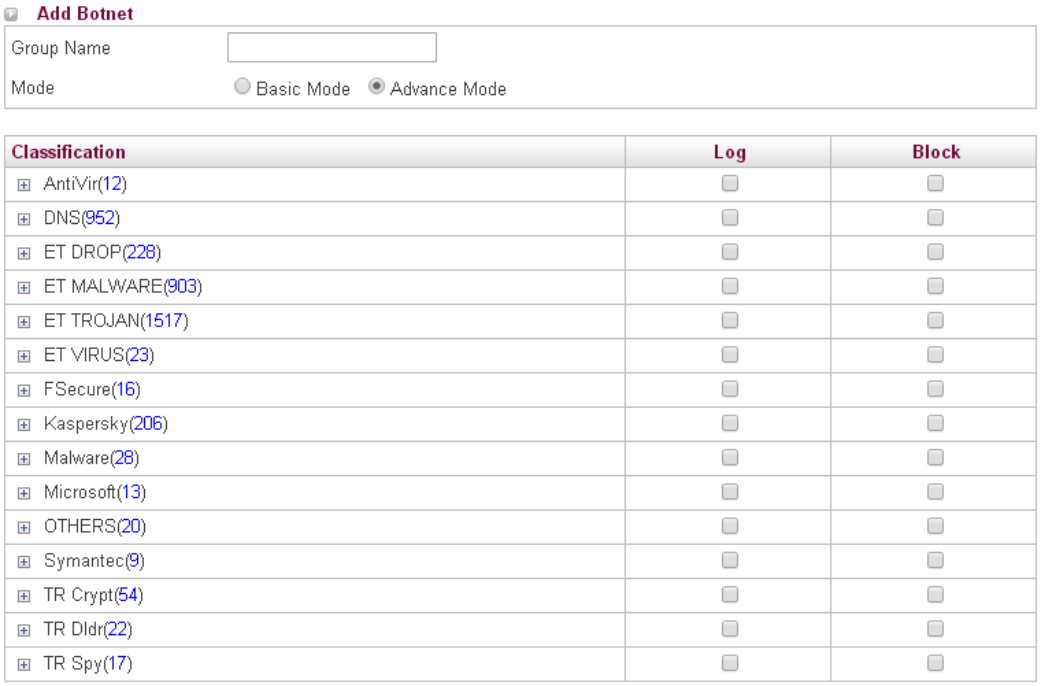
Select *IDP & BotNet > BotNet Setting > BotNet Filter Setting*.

BotNet traffic filtering have been classified into 2 modes - basic and advanced. In the basic mode, signatures are organized into 3 levels- High risk, medium risk, and low risk. Administrators can check to activate log or blocking according to business needs.

Ps. Sniffer Mode cannot enable blocking.

In the advanced mode, Administrators can check to activate log or blocking according to business needs based on various signature categories.

Ps. Sniffer Mode cannot enable blocking.



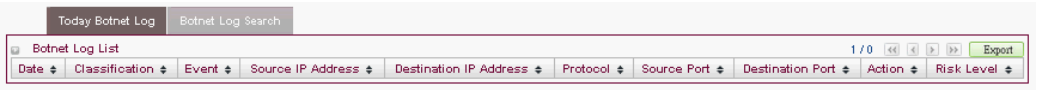
9.4 BotNet Log

9.4.1 Today BotNet Log

Select *IDP & BotNet > BotNet Log > Today BotNet Log*.

Today BotNet Log displays violations based on date, classification, event, source IP address, destination IP address, protocol, source port, destination port, action and risk level.

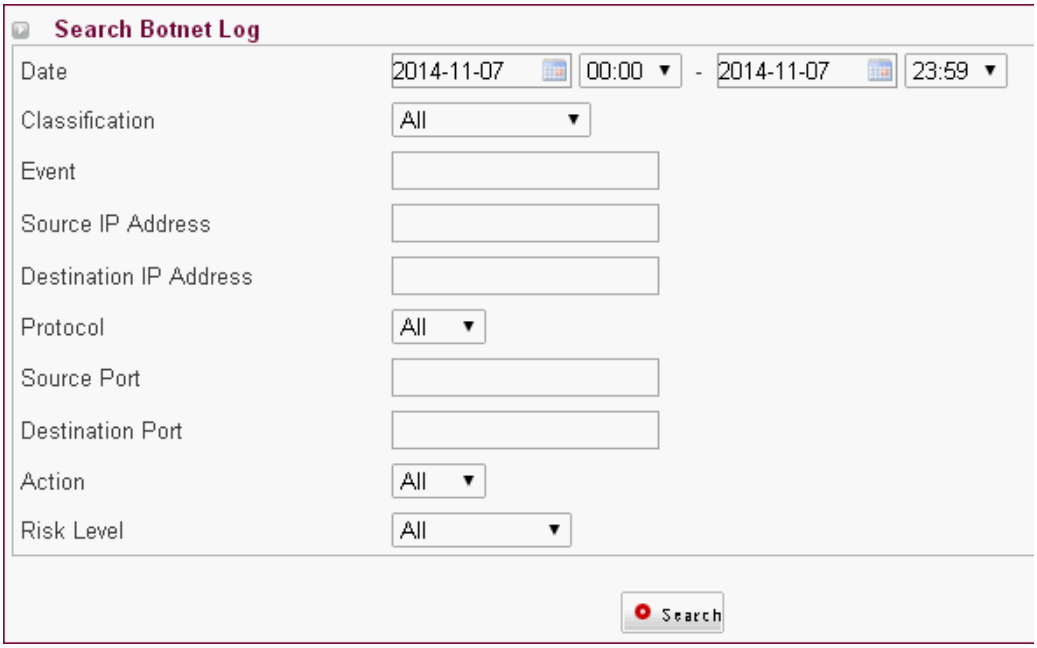
You may click on to list out all the items, see figure below.



9.4.2 BotNet Log Search

Select *IDP & BotNet > BotNet Log > BotNet Log Search*.

BotNet Log Search provides various searching conditions such as date, classification, event, source IP address, destination IP address, protocol, source port, destination port, action and risk level.



This page is intentionally left blank.

Chapter 10
SSL VPN

Since the Internet is in widespread use these days, the demand for secure remote connections is increasing. To meet this demand, using SSL VPN is the best solution. Using SSL VPN and just a standard browser, clients can transfer data securely by utilizing its SSL security protocol, eliminating the need to install any software or hardware.

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard web browser. In contrast to the traditional Internet Protocol Security (IPSec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to web applications, client/server applications and internal network connections. A virtual private network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints. An SSL VPN consists of one or more VPN devices to which the user connects by using his web browser. The traffic between the web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) Protocol.

An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations. There are two major types of SSL VPNs:

1. SSL Portal VPN: This type of SSL VPN allows for a single SSL connection to a website so the end user can securely access multiple network services. The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any modern web browser, identifies himself or she to the gateway using an authentication method supported by the gateway and is then presented with a web page that acts as the portal to the other services.
2. SSL Tunnel VPN: This type of SSL VPN allows a web browser to securely access multiple network services, including applications and protocols that are not web-based, through a tunnel that is running under SSL. SSL tunnel VPNs require that the web browser be able to handle active content, which allows them to provide functionality that is not accessible to SSL portal VPNs.

In this SSL VPN chapter you can enable the following lists:

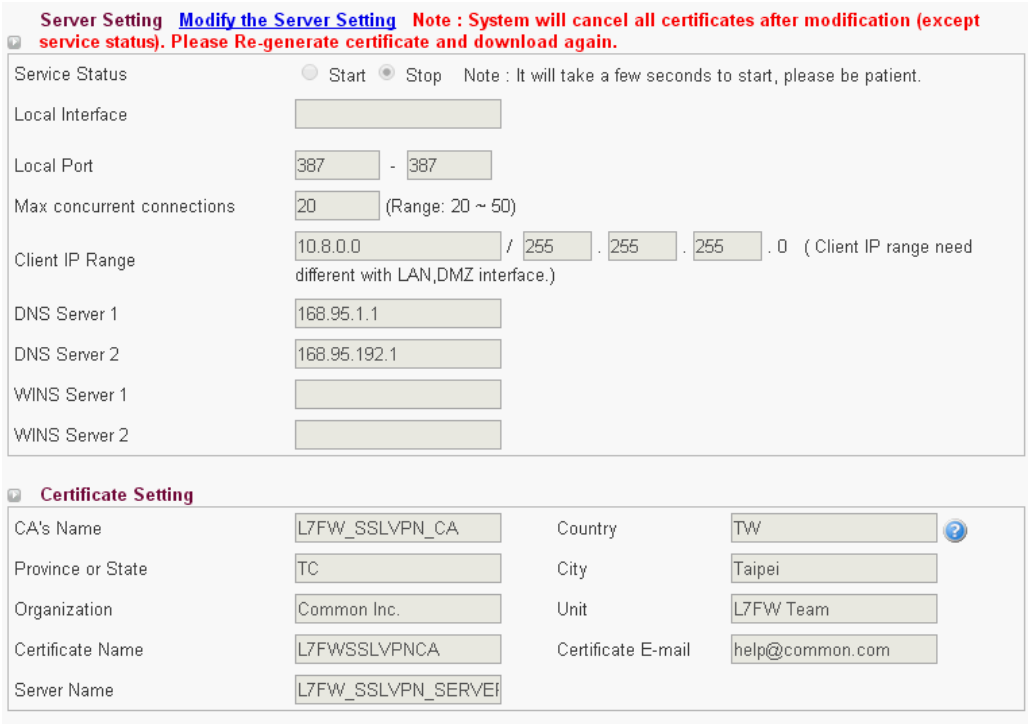
- SSL VPN Setting
- SSL VPN Log
- VPN Policy

10.1 SSL VPN Setting

10.1.1 SSL VPN Setup

Users have to click on “Modify the Server Setting” link, to modify SSL VPN settings. In addition, users must select “Start” because default setting is “Stop”.

Note that system will cancel all certificates after modification (except service status). Please re-generate certificate and download again.



Service Status
Select “Start”/”Stop” to start/stop this function. Note that it will take a few seconds to start, please be patient.

Local Interface
1. Default
2. Custom
3. WAN

Local Port
Default setting is 387.

Max concurrent connections
Range from 20~50.

Client IP Range
Client IP ranges need to be different from LAN interface.

DNS Server 1
The IP address of the DNS server used for the bulk of DNS lookups.

DNS Server 2
The IP address of the backup DNS server, used when the Primary DNS server is unreachable.

WINS Server 1
Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

WINS Server 2
All WINS clients should be configured to use a primary WINS server and a different secondary WINS server. The secondary would normally be the hub server.

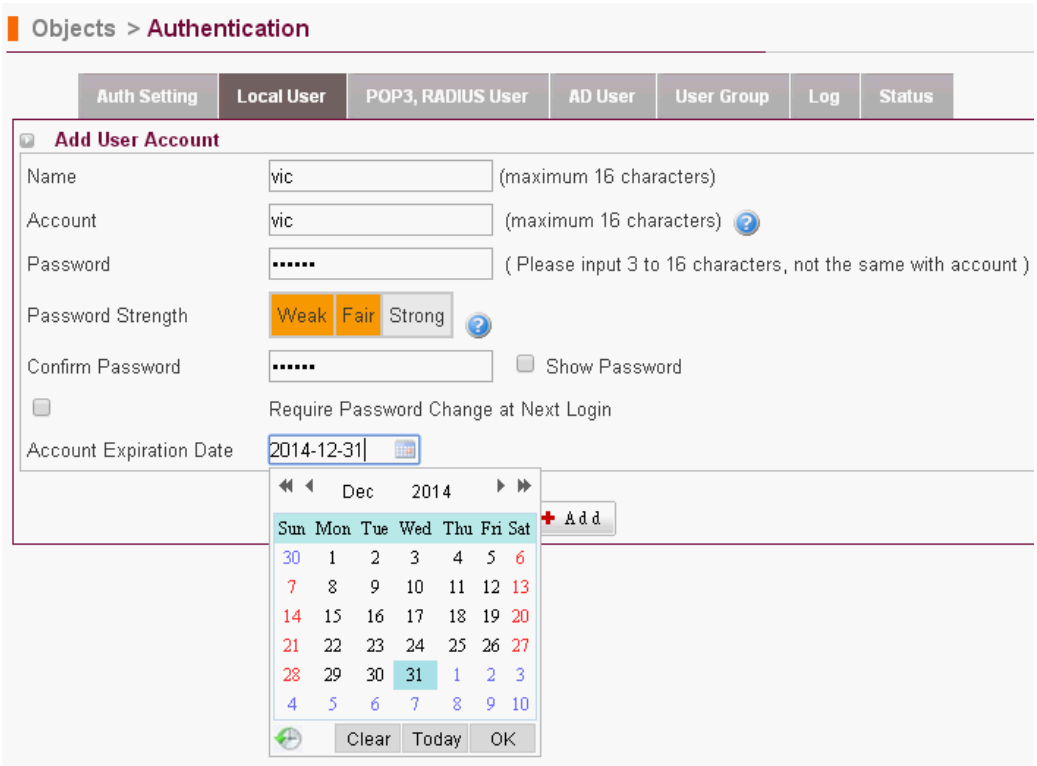
Certificate Settings
Enter your computer certificate information for SSL VPN users.

Do not forget to select "Start" to begin SSL VPN.

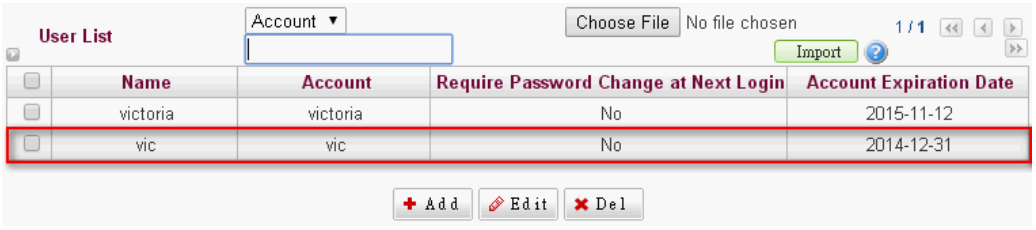
10.1.2 SSL Client List

Please create an account in *Objects* > *Authentication* > *Local User*.

Create authentication account:

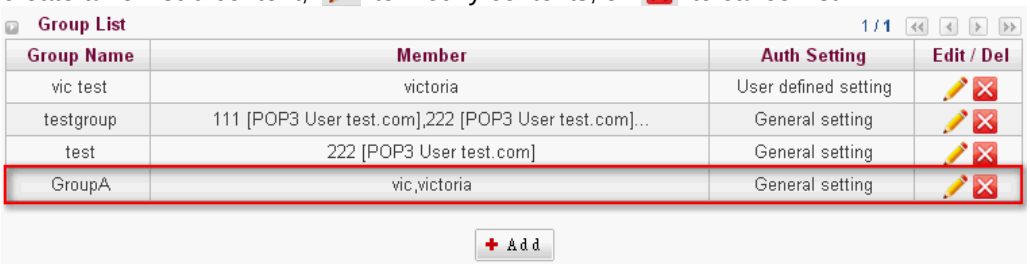


Authentication user list:

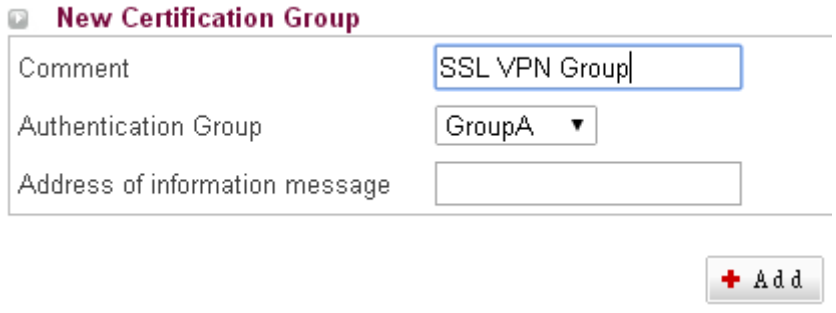


Then, select *Objects* > *Authentication* > *User Group*. Click on Add to create a new Authentication User Group.

Setting User Group with Local Users mode completed. In addition, click on Add to create a new sub-content, to modify contents, or to cancel list.

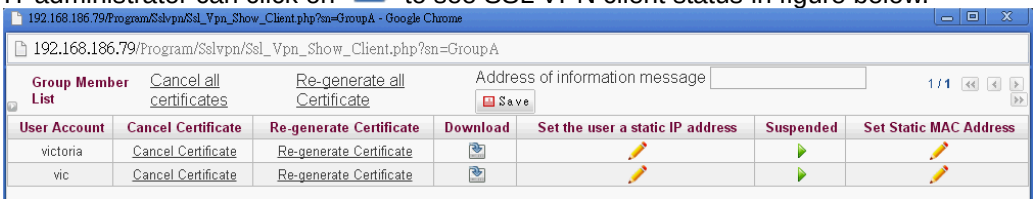


Then, go to *SSL VPN* > *SSL VPN Setting* > *SSL Client List*. Please click on Add to create a new certification Group.



Setting SSL VPN Client with Authentication Local Users completed, see figure below.

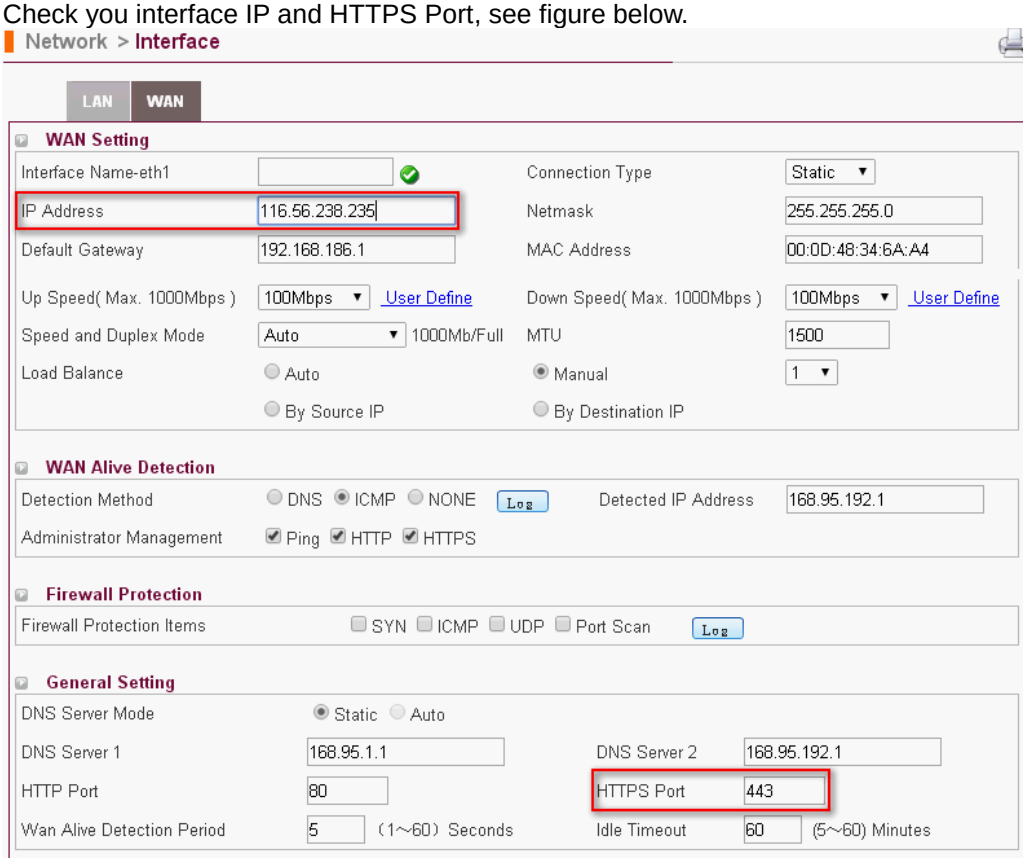
IT administrator can click on to see SSL VPN client status in figure below.



User should download generated certificate into their computer, laptop, or iPad by using https:// [WAN IP Address or Domain] : [HTTPS Port] /sslvpn.php.

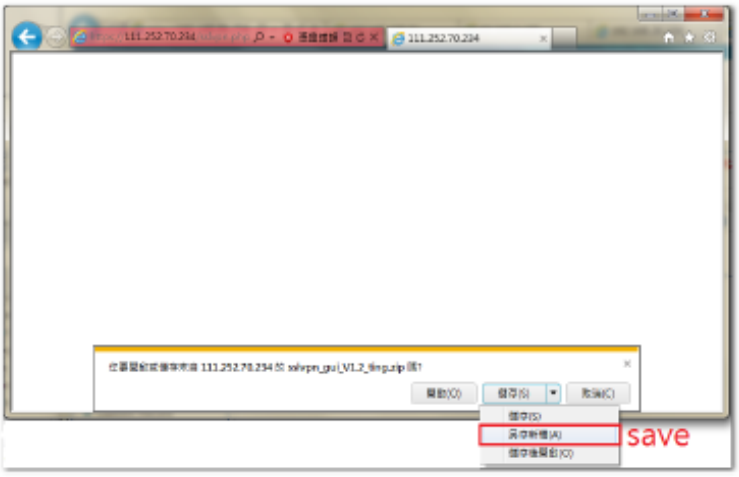
For example, https://116.56.238.235:443/sslvpn.php.

Check you interface IP and HTTPS Port, see figure below.

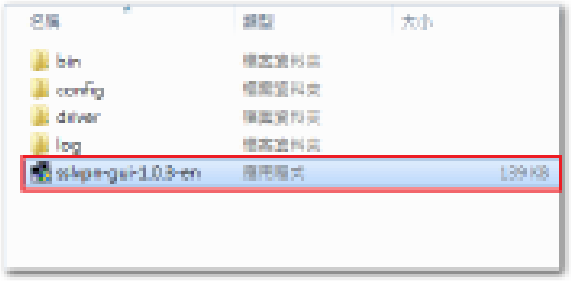


Enter https://116.56.238.235:443/sslvpn.php in your browser, and then enter your user account and user password.

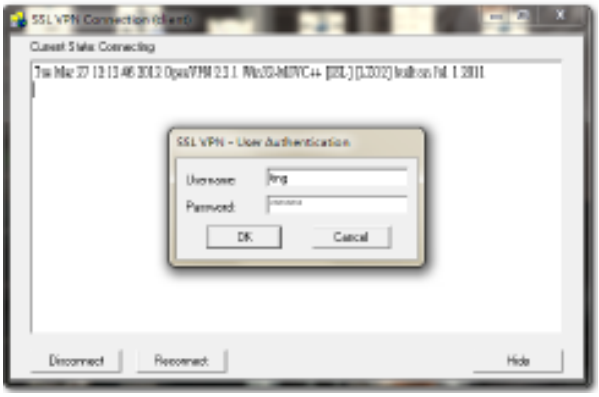
Download generated certificate into your computer, laptop, or iPad.



Open .zip file (see figure below). Or update your driver (choose tap-win32 or tap-win64).



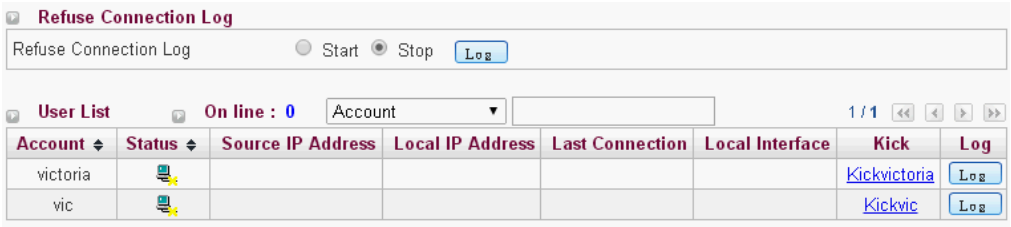
Then, click on, and enter your username and password. The figure below shows SSL VPN Connection (Client) screen.



10.2 SSL VPN Log

10.2.1 SSL Client On-Line Log

Select *SSL VPN > SSL VPN Log >SSL Client On-Line Log*.



Refuse Connection Log
Select "Start"/"Stop" to start/stop this function.

In addition, you can click on Log to see SSL VPN logs.

10.3 VPN Policy

This section is the same as section 11.4 VPN Policy. In this section you can enable the following lists:

- Internal to VPN
- VPN to Internal

SSL VPN on internal control and external control through the SSL VPN connection points connected to internal network, the Protocol, Service group port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis. Select *SSL VPN > VPN Policy > VPN to Internal or Internal to VPN*.

Click on + Add
Create a new VPN policy. VPN's policy is as follows, policies started from the priority1, will be the implementation of eligible project. If you want to ban non-control information into the internal network, it will need to last a total of all the packets into the internal prohibited.

Policy Name
Enter any word for recognition.

Source Address and Destination
Source Address (source network) and Destination Address (the destination network) are for the observation points, connect one end of the active source network address, be connected to one end of the network address for the purpose of, apart from the policy choices, users can also directly enter the IP address and MAC address.

1. Source IP address: VPN_Any will be the representative of the external section of all VPN tunnels, either with IPSec, PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The default IP address of the PPTP server will also be included in the default source IP address.
2. The destination IP Address: Inside_Any will be the representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The demand for network administrators can allow or deny specific VPN access other end of the incoming IP address, communication services and even time. The default access control rule is when the VPN is established, both materials are free to communicate with each other to exchange, unless prohibited it from incoming VPN controls.

Action
It offers two movements
1. ACCEPT means any meet the Policy of the packet will be released.
2. Drop means discarded.

Protocol
The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others

Service group Port or Group
With service groups, the administrator in setting policy can simplify many processes.

Example

For example, there are ten different IP addresses on the server can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service group functions, you need to develop a total of 10x5=50 policies. But with the use of service group functions, you only need a policy to achieve the function of 50.

QoS
Select *Objects* > *QoS*. Then, the VPN policy set the maximum bandwidth and rate bandwidth (Bandwidth is consistent with the policy of the user to share).

Schedule
Select *Objects* > *Schedule*. Then, set your schedule time.

Packet tracing
Select “Packet tracing” tick box to start function. It records all packets passing through VPN tunnel.

Traffic Analysis
Select “Traffic Analysis” tick box to start function.

Chapter 11
VPN

To obtain a private and secure network link, the IFW320 is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secures options for enterprises to adopt in comparison to other methods. In this VPN chapter you can enable the following lists:

- IPSec Tunnel
- PPTP Server
- PPTP Client
- VPN Policy

11.1 IPSec Tunnel

IPSec (IPSec = IP Security) is a generic standardized VPN solution. IPSec must be implemented in the IP stack which is part of the kernel. Since IPSec is a standardized protocol it is compatible to most vendors that implement IPSec. It allows users to have an encrypted network session by standard IKE (IKE = Internet Key Exchange). We strongly encourage you to use IPSec only if you need to because of interoperability purposes.When IPSec lifetime is specified, the device can randomly refresh and identify forged IKE's during the IPSec lifetime. In this section you can enable the following lists:

11.1.1 IPSec Tunnel

Select *VPN* > *IPSec Tunnel* > *IPSec Tunnel*. Click on

button to create a new IPSec Tunnel.

Enabled
Select it to start the connection.

IPSec Tunnel Name
Enter any words for recognition.

Interface
This is only available for host-to-host connections and specifies to which interface the host is connecting.

Remote IP Address
The IP or fully qualified domain name of the remote host.
1. IP Address or Domain: Enter an IP Address or Domain.
2. Dynamic: Follow Dynamic IP address.

Local Subnet
The local subnet in CIDR notation.

Example

For instance, "192.168.15.0/24".

Remote Subnet
This is only available for net-to-net connections and specifies the remote subnet in CIDR notation.

Example

For instance, "192.168.16.0/24".

Connection Type
There are two types.
1. Main
2. Aggressive

Preshare Key
Enter a pass phrase to be used to authenticate the other side of the tunnel.

ISAKMP (ISAKMP = Internet Security Association Key Management Protocol)
It provides the way to create the SA (SA = Security Association) between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign of which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.
1. AES (AES = Advanced Encryption Standard): All using a 128-bit, 192-bit and 257-bit key. AES is a commonly seen and adopted nowadays.
2. 3DES (DES = Data Encryption Standard): Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.
3. SHA1: The SHA1 is a revision of SHA (SHA = Secure Hash Algorithm). It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.
4. MD5 (MD5 = Message Digest Algorithm) Algorithm: MD5 processes a variable-length message into a fixed–length output of 128 bits.
5. DH Group: When the encryption technique is aes, it can be choice 2, 5, 14, 15, 16, 17, 18, but if the encryption technique is 3des, it only can be choice 2, 5.
6. Auto Pairing

Local ID
An ID for the local host of the connection.

Remote ID
An ID for the remote host of this connection

IKE SA Lifetime
You can specify how long IKE packets are valid.

IPSec
It offers aes, 3des, sha1, and md5.

1. AES: All using a 128-bit, 192-bit and 257-bit key. AES is a commonly seen and adopted nowadays.
2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.
3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.
4. MD5 Algorithm: MD5 processes a variable-length message into a fixed–length output of 128 bits.
5. Auto Pairing

Perfect Forward Secrecy (PFS = Perfect Forward Secrecy)
Set “Yes” to start the function. DH Group, when the encryption technique is aes, it can be choice2, 5, 14, 15, 16, 17, 18, but the encryption technique is 3des, only can be choice 2 , 5.

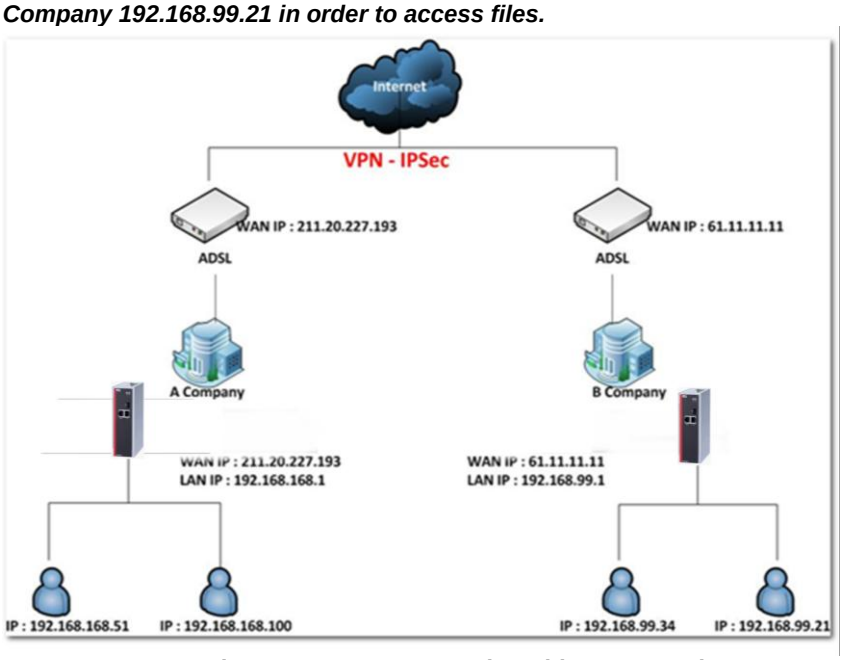
IPSec SA Lifetime
Set to 1~3 hours. Default setting is 3 hours.

Dead Peer Detection
When starting DPD function, when VPN detects opposite party reaction time, “Hold” stands for the system will retain IPSec SA, "Clear" stands for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPSec SA and reset VPN tunnel.

Drop SMB Protocol
After the closure Network Neighborhood will be prevented.

Example

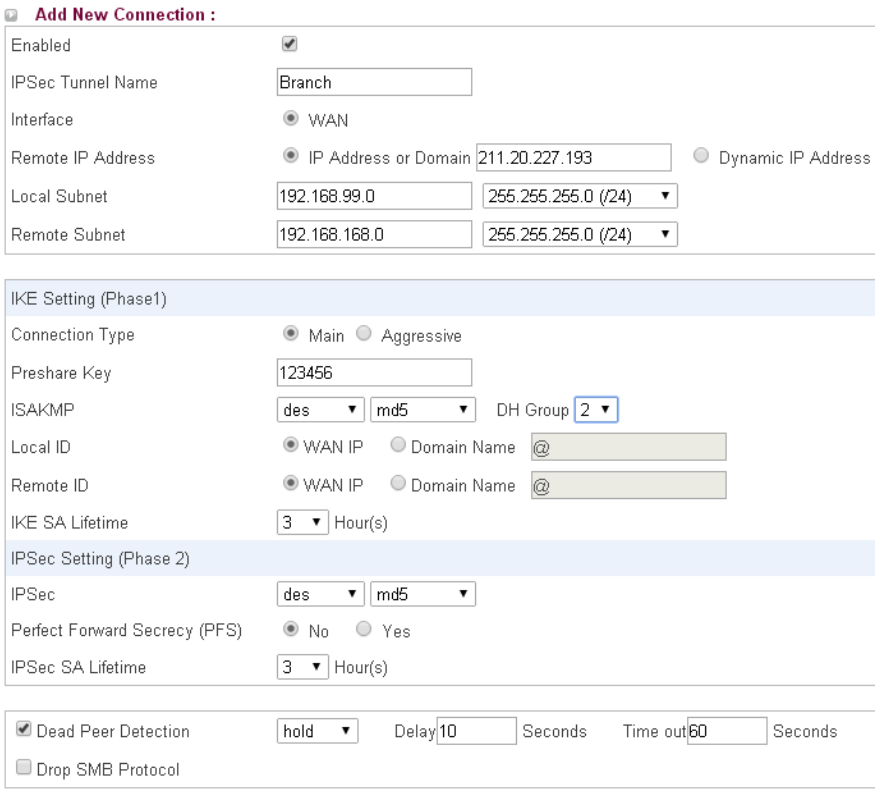
Here is an example showing how to utilize two IFW320 devices. Assume that A Company 192.168.168.51 wants to create a VPN connection with B Company 192.168.99.21 in order to access files.



For A company: Select VPN > IPSec Tunnel > Add VPN Tunnel. Its WAN IP is 211.20.227.193, and LAN subnet is 192.168.168.0/24. Default gateway for the A company LAN IP 192.168.168.1.

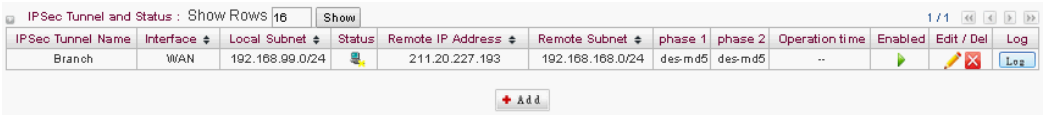
1. ***VPN Tunnel Name: Enter "VPN_B" in the field.***
2. ***Interface: Select "WAN." (Suggest using static IP).***
3. ***Local Subnet: Enter "192.168.168.0 255.255.255.0 (/24)"***
4. ***Remote Subnet: Enter "192.168.99.0 255.255.255.0 (/24)"***
5. ***Preshare Key: Enter numbers for B Company. Should be the same with B Company (The maximum length of Preshare key is 103 characters).***
6. ***ISAKMP: Select "aes" and "sha1," and set "DH Group".***
7. ***Local ID: Default is using WAN IP Address as ID, administrator also can use domain as ID. For example "@1.1.1.1" or "@abc.com".***
8. ***Remote ID: Used in the same way as Local ID.***
9. ***IKE SA Lifetime: The default is 3 hours. After IKE establishment surpasses the system set time, a new IKE will be produced.***
10. ***IPSec: Select "aes" and "md5" for IPSec. And select Auto Pairing to start. To start Auto Pairing, the system's all calculation combination will converge in the rule, If IFW320 = SERVE, the same combination will be discovered automatically on behalf of the system with the far-end segment.***
11. ***Perfect Forward Secrecy (PFS): Set to "Yes". (The default setting is not working), and select DH Group.***
12. ***IPSec SA Lifetime: Set to 1~3 hours. The default setting is 3 hours.***
13. ***Dead Peer Detection: Set up the detection time of DPD, the DPD detection's gap is 30 seconds, over 300 seconds to think that is the broken line.***
14. ***Drop SMB Protocol: After the closure Network Neighborhood will be prevented.***
15. ***Settings completed.***

For B Company: B Company setting steps is similar to A Company setting. WAN IP is 61.11.11.11, LAN subnet is 192.168.99.0/24. Figure below shows how to Add IPSec Tunnel for B company.



11.1.2 Add IPSec Tunnel

Setting IPSec Tunnel completed, and please notices the status.



VPN and Status:

1. Interface: At present IPSec VPN use entity interface; WAN.

2. Status:
   a. : The VPN is not work.
   b. : The VPN is on work.

3. Enabled: Control IPSec VPN start and suspension button.
   a. : Stand for start.
   b. : Stand for suspension.

4. : Stand for editing the VPN setting.

5. Log: This VPN communication record, IPSec VPN channel, if has the communication record with opposite party, select the Log will open the new Windows, the data will be according to time sorting, most recent news in last page.

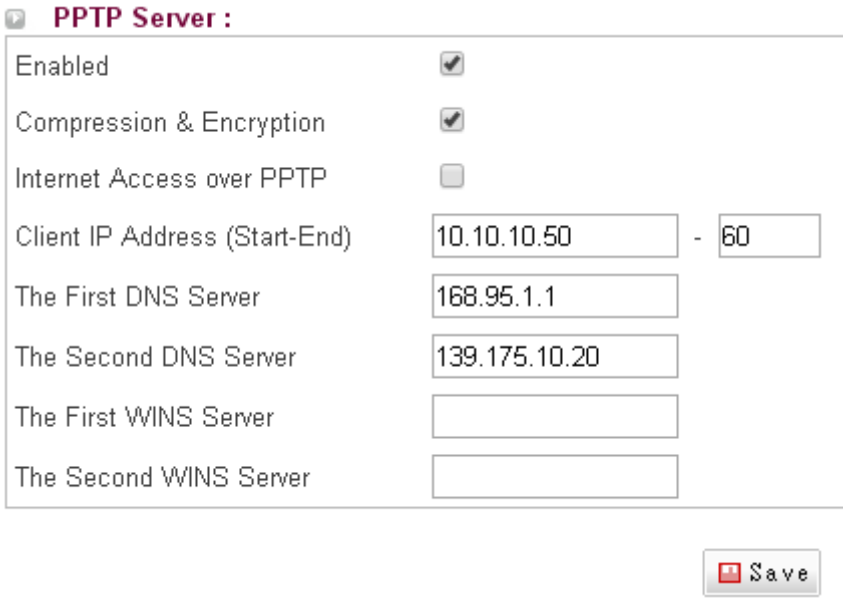
11.2 PPTP Server

This section shows you how to set VPN-PPTP server. Uses the IP address and the scope option needs to match the far-end PPTP server. Its goal is to use the PPTP channel technology, to establish Site to Site VPN. This function gives the meaning of equally good results obtained from other methods besides IPSec. In this section you can enable the following lists:

11.2.1 PPTP Server

Enabling IFW320 PPTP Server allows remote user to use PPTP dial-up software to establish encrypted VPN connection.

Select *VPN > PPTP Server > PPTP Server*.



Enabled
Select “Enabled” tick box to start VPN-PPTP function. Or otherwise, if not selected, it will be disabled.

Enable Compression & Encryption
Select “Enabled” tick box to start compression and encryption. Or otherwise, if not selected, it will be disabled.

Internet Access over PPTP
Select tick box to enable user who pass through Internet by VPN-PPTP, or otherwise, it means that PPTP Server is disabled.

Client IP Address (Start-End)
The range of IP address for clients using PPTP connection.

The first DNS Server
The IP address of the DNS server used for the bulk of DNS lookups.

The second DNS Server
The IP address of the backup DNS server, used when the Primary DNS server is unreachable.

The first WINS Server
When the PPTP clients enter the PPTP Server, assigns for the far-end client WINS Server address.

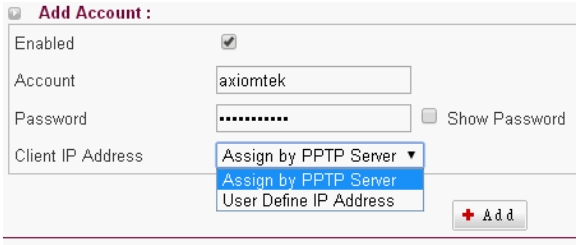
The second WINS Server
When the PPTP clients enter the PPTP Server, assigns for the far-end client WINS Server address.

Click on

Start PPTP Server.

11.2.2 Add Account

Select *VPN > PPTP Server > Add Account*.



Enabled
Select “Enabled” to start this account.

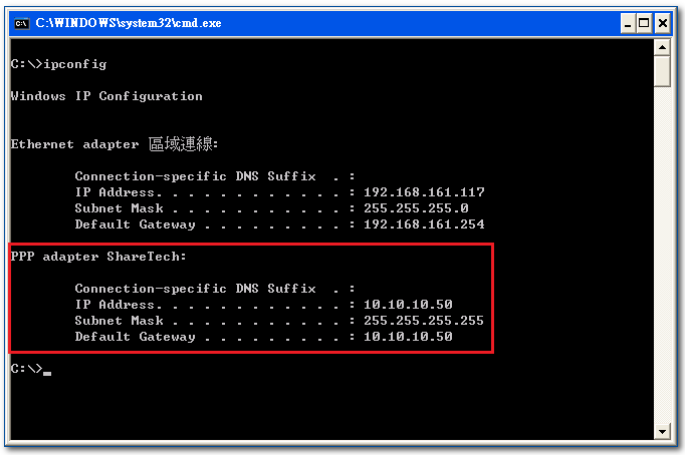
Account
Enter an account.

Password
Enter a password.

Client IP Address Assign
It offers three ways.

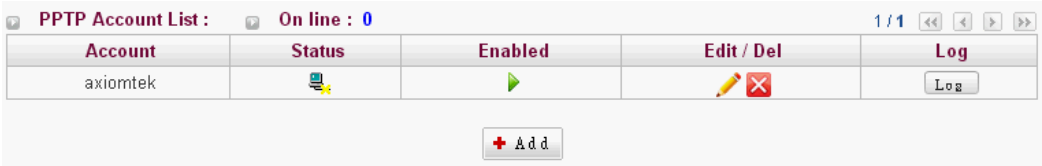
1. Use Allocation IP Address: The IFW320 will distribute IP address to the VPN-PPTP users automatically.
2. User Enter IP Address: The VPN-PPTP users should use the IP address you enter.
3. Enter IP Address and Range: The VPN-PPTP users should use range of the IP address you enter.

Check IP address after connecting to PPTP:


C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter 區域連線:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.161.117
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.161.254
PPP adapter ShareTech:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.10.10.50
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 10.10.10.50
C:\>

11.2.3 PPTP Account List

Select *VPN* > *PPTP Server* > *PPTP Account List*. After setting PPTP account completed, you can see the following list.



Account
Available VPN-PPTP account.

Status
The symbol and its description used in the VPN connection status.

1. : It is connecting.
2. : Disconnected.

Enabled
Click on again and it will change to .

1. : Enable
2. : Disable

Edit / Del
Click on the pencil signature to modify contents, and click on to delete PPTP account.

1. : Modify contents
2. : Delete PPTP account

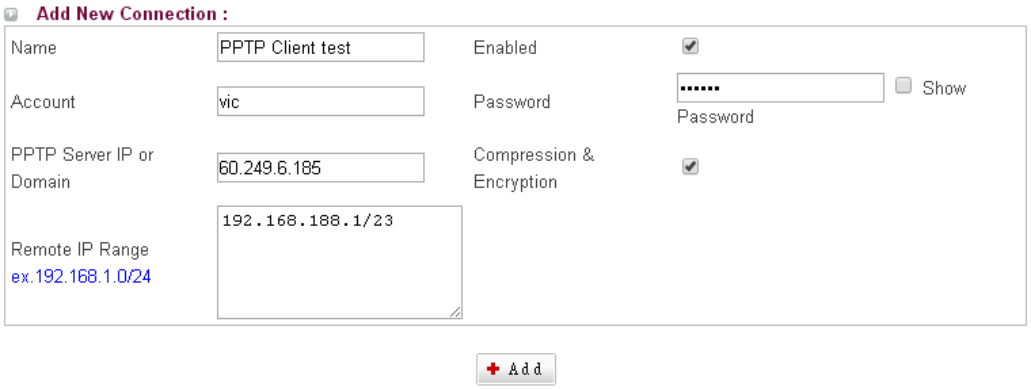
Log
Click on Log to show the PPTP account connection logs.

11.3 PPTP Client

In the PPTP Client section you can enable the following lists:

11.3.1 Add PPTP Client

Select *VPN* > *PPTP Client* > *Add PPTP Client*.



Name
The description for PPTP Client.

Account
It displays the name of clients using PPTP to log in to PPTP server.

PPTP Server IP or Domain
Enter a server IP address.

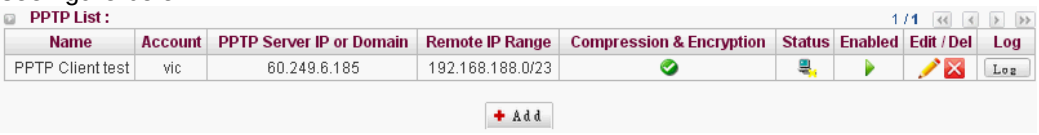
Remote IP Range
Enter the range of remote IP address.

Enabled
Select it to start PPTP Client account.

Password
It displays the password of clients using PPTP to log in to PPTP server.

11.3.2 PPTP Client List

Select *VPN* > *PPTP Client* > *PPTP Client List*. It means setting PPTP Client is completed, see figure below.



11.4 VPN Policy

The intelligence and power behind the Positive Networks VPN service derives from the Positive VPN Policy Manager. The Positive VPN Policy Manager provides the administrator interface that maintains and enforces security policies for all groups and individual users. It is available from an ordinary web browser with a secure login. To create a secure VPN connection, the settings of IPSec Tunnel, PPTP Server or PPTP Client must be set to correlative policies.

Caution

The default of VPN Policy does not grant pre-control. As long as the VPN connection is established successful, the two-way computer can communicate, if only the control of the target was expected through the proposed regulations in the last one against all connections.

11.4.1 Internal to VPN and VPN to Internal

The control of the VPN in the past, most were carried out from the policies or is unable to monitor. IFW320 for the VPN is direct control from the VPN. VPN on internal control and external control through the VPN connection points connected to internal network, the Protocol, Service port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis. Select *VPN > VPN Policy> VPN to Internal or Internal to VPN*.

Click on

Create a new VPN policy. VPN's policy is as follows, policies started from the priority1, will be the implementation of eligible project. If you want to ban non-control information into the internal network, it will need to last a total of all the packets into the internal prohibited.

Policy Name
Enter any word for recognition.

Source Address and Destination
Source Address (source network) and Destination Address (the destination network) are for the observation points, connect one end of the active source network address, be connected to one end of the network address for the purpose of, apart from the policy choices, users can also directly enter the IP address and MAC address.

1. Source IP address: VPN_Any will be the representative of the external section of all VPN tunnels, either with IPSec, PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The default IP address of the PPTP server will also be included in the default source IP address.
2. The destination IP Address: Inside_Any will be the representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The demand for network administrators can allow or deny specific VPN access other end of the incoming IP address, communication services and even time. The default access control rule is when the VPN is established, both materials are free to communicate with each other to exchange, unless prohibited it from incoming VPN controls.

Action
It offers two movements

1. Permit means any meet the Policy of the packet will be released.
2. Drop means discarded.

Protocol
The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others

Service group Port or Group
With service groups, the administrator in setting policy can simplify many processes.

Example

For example, there are ten different IP addresses on the server can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service group functions, you need to develop a total of 10x5=50 policies. But with the use of service group functions, you only need a policy to achieve the function of 50.

QoS
Select *Objects* > *QoS*. Then, the VPN policy set the maximum bandwidth and rate bandwidth (Bandwidth is consistent with the policy of the user to share).

Schedule
Select *Objects* > *Schedule*. Then, set your schedule time.

Packet tracing
Select “Packet tracing” tick box to start function. It records all packets passing through VPN tunnel

Traffic Analysis
Select “Traffic Analysis” tick box to start function.

This page is intentionally left blank.

Chapter 12
Tools

In this Tools chapter you can enable the following lists:

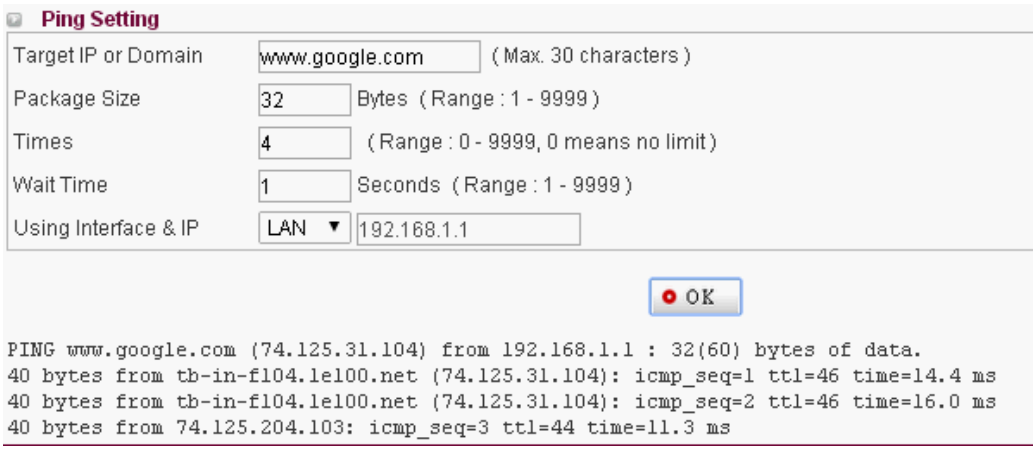
- Connection Test
- Remote Management

12.1 Connection Test

In this section, IFW320 provides Ping, Traceroute, DNS Query, Port Scan, IP Route, Interface Information and Wake up utilities to help diagnose network issues with particular external nodes.

12.1.1 Ping

It is an ICMP protocol. Most people usually use ping to diagnostic Internet between self and other people when Internet disconnected. Select *Tools* > *Connection Test* > *Ping*. Enter some information in the field, and click on OK. Then, you will see Ping Result.


Ping Setting
Target IP or Domain
www.google.com
(Max. 30 characters)
Package Size
32
Bytes (Range : 1 - 9999)
Times
4
(Range : 0 - 9999, 0 means no limit)
Wait Time
1
Seconds (Range : 1 - 9999)
Using Interface & IP
LAN
192.168.1.1
OK
PING www.google.com (74.125.31.104) from 192.168.1.1 : 32(60) bytes of data.
40 bytes from tb-in-f104.1e100.net (74.125.31.104): icmp_seq=1 ttl=46 time=14.4 ms
40 bytes from tb-in-f104.1e100.net (74.125.31.104): icmp_seq=2 ttl=46 time=16.0 ms
40 bytes from 74.125.204.103: icmp_seq=3 ttl=44 time=11.3 ms

Target IP or Domain
Enter the Target IP or Domain name in this field.

Package Size
It configures the size of each packet. Default setting is 32Bytes.

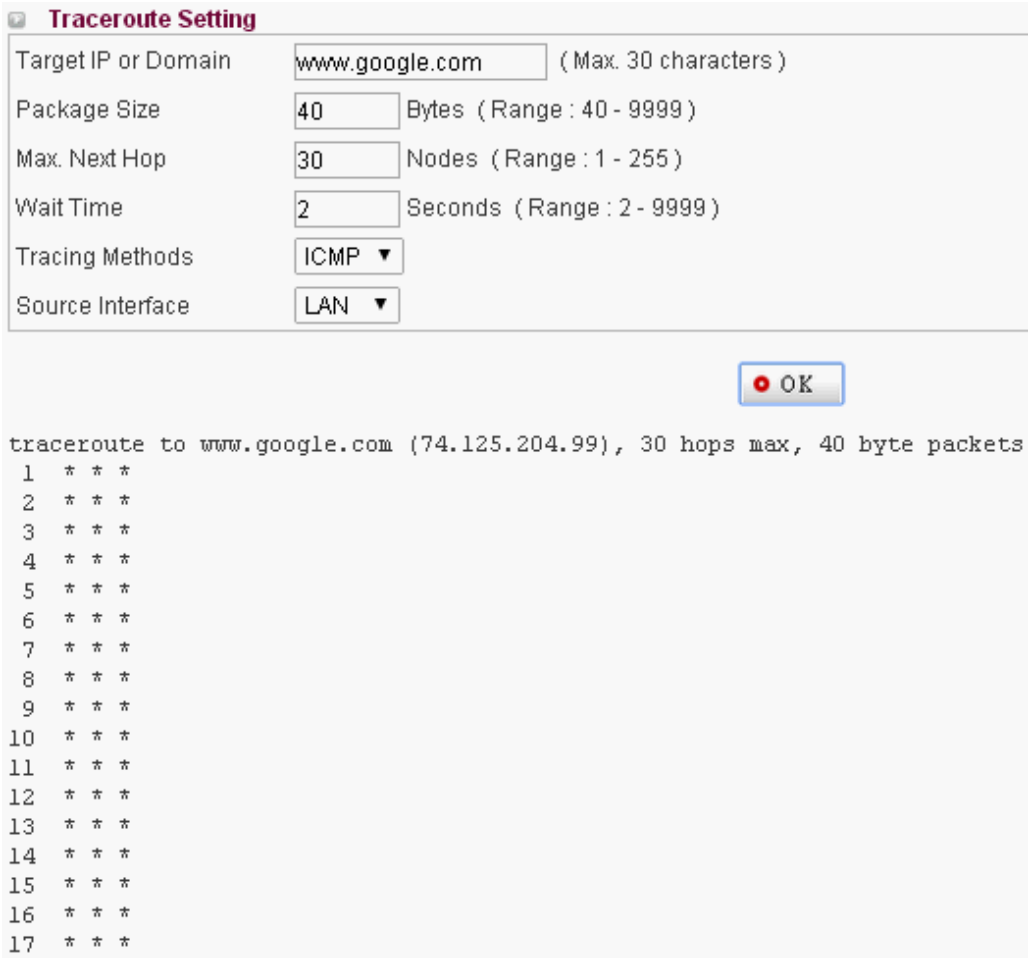
Times
It configures the quantity of packets to send out. Default setting is 4.

Wait Time
It specifies the duration to wait between successive pings. Default setting is 1 second.

Using Interface & IP
Select an interface. There are LAN and WAN.

12.1.2 Traceroute

Traceroute command can be used by the IFW320 to send out packets to a specific address to diagnose the quality of the traversed network. Select *Tools* > *Connection Test* > *Traceroute*. Enter some information in the field, and click on OK. Then, you will see Traceroute Result.



Target IP or Domain
Enter the destination address for the packets.

Package Size
Configure the size of each packet. Default setting is 40 Bytes.

Max. Next Hop
Enter the maximum number of hops. Default setting is 30 Nodes.

Wait Time
Specify the duration to wait between successive pings. Default setting is 2 seconds.

Tracing Methods
There are ICMP, UDP, and TCP.

Source Interface
Select the interface that the packets will originate from. There are LAN and WAN.

12.1.3 DNS Query

Query DNS detailed data which include ANY, SOA, NS, A Record, MX, CNAME, PTR from local host IFW320 or specific DNS server.

Select *Tools* > *Connection Test* > *DNS Query*. Enter some information in the field, and click on OK. Then, you will see DNS Query Result.

Using DNS Server
Enter a DNS server IP address or domain name in this field. (Max. 50 Characters).

Domain or IP to Query
Enter an IP address or domain name in this field. (Max. 50 Characters).

Query Type
Select the interface from the list. There are ANY, SOA, NS Record, A Record, MX Record, CHAME, and PTR.

12.1.4 Port Scan

To inquire the Port Scan detailed material, which at present can inquire the server to open to serve the port, contains FTP, SSH, TELNET, SMTP, DNS, HTTP, POP3, SAMBA, IMAP, SNMP, PROXY, MySQL, SMTPS, IMAPS…etc.

Select *Tools* > *Connection Test* > *Port Scan*. Enter domain or IP address for the packets in the field, and click on OK. Then, you will see Port Scan Result.

Port Scan Setting

Domain or IP to Scan 192.168.188.139 (Max 50. characters)

OK

Port Scan Result

10:48:41 FTP====>> FAIL

10:48:42 SSH====>> FAIL

10:48:43 TELNET====>> FAIL

10:48:44 SMTP====>> FAIL

10:48:45 HTTP====>> FAIL

10:48:46 POP3====>> FAIL

10:48:47 SAMBA====>> FAIL

10:48:48 IMAP====>> FAIL

10:48:49 SNMP====>> FAIL

10:48:50 PROXY====>> FAIL

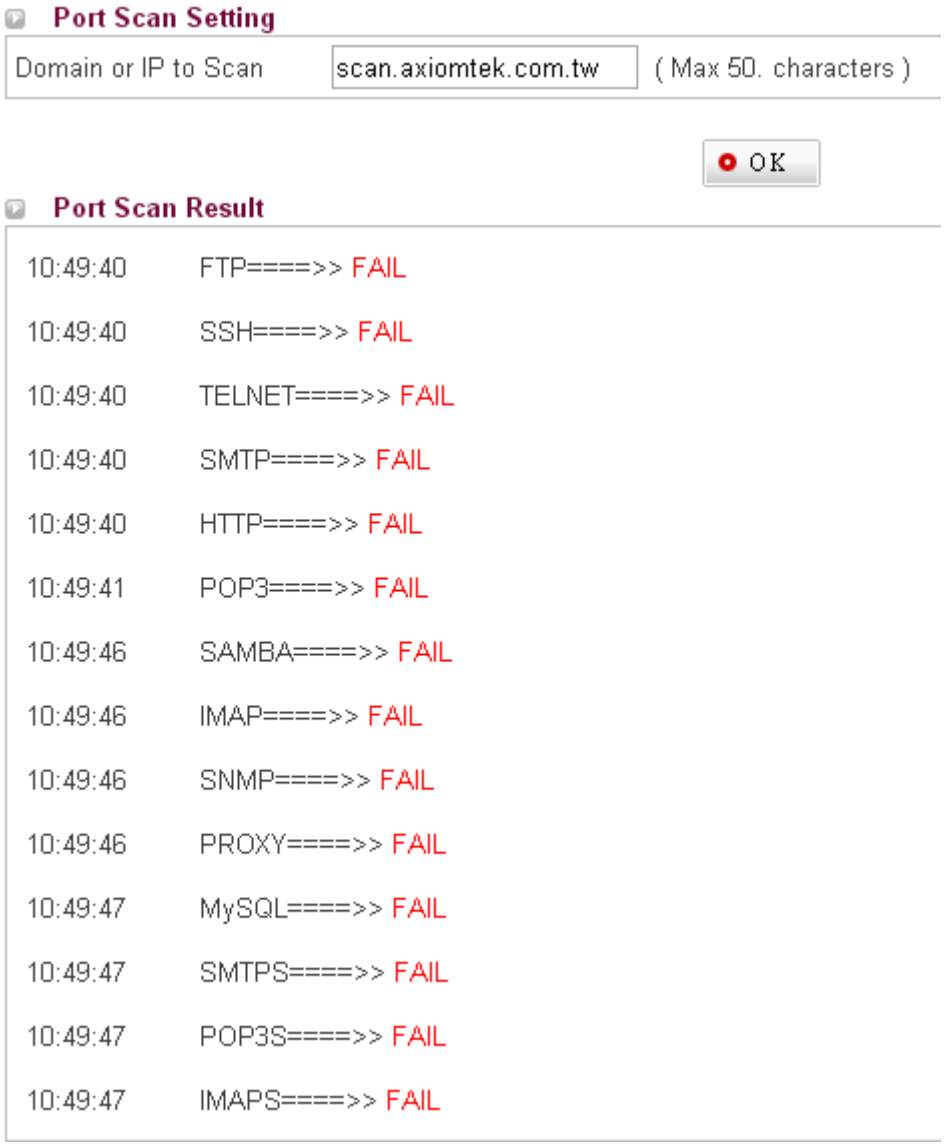
10:48:51 MySQL====>> FAIL

10:48:52 SMTPS====>> FAIL

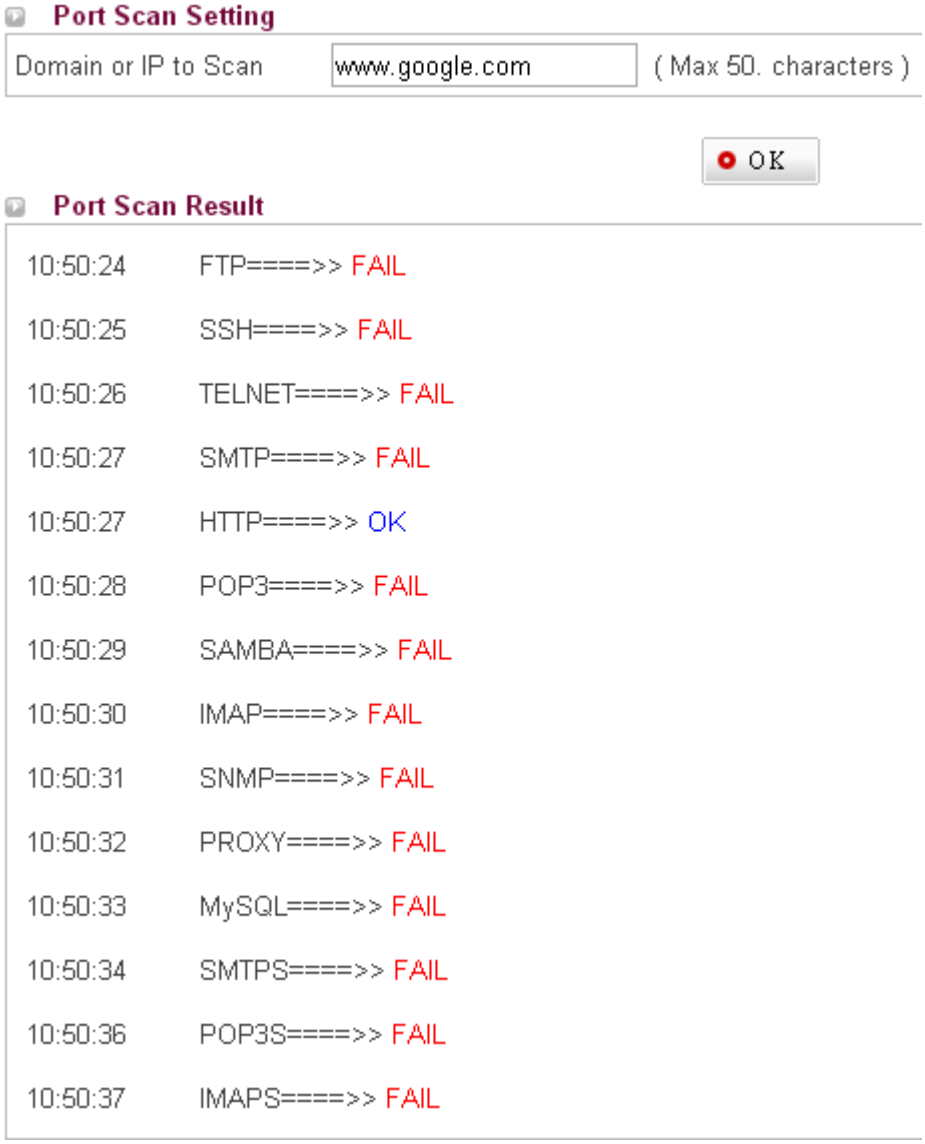
10:48:53 POP3S====>> FAIL

10:48:54 IMAPS====>> FAIL

Scanning www.axiomtek.com.tw:

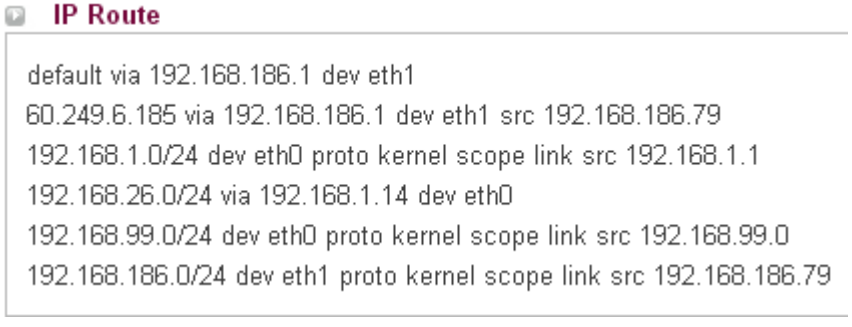


Scanning www.google.com:



12.1.5 IP Route

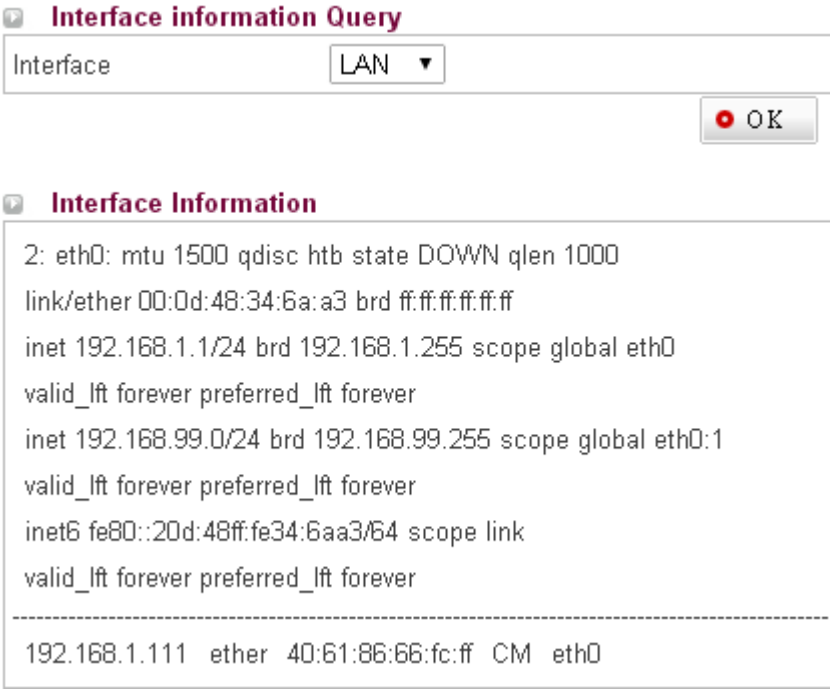
IP Route shows router status in order to know router information; it also shows multiple subnet status.


IP Route
default via 192.168.186.1 dev eth1
60.249.6.185 via 192.168.186.1 dev eth1 src 192.168.186.79
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.1
192.168.26.0/24 via 192.168.1.14 dev eth0
192.168.99.0/24 dev eth0 proto kernel scope link src 192.168.99.0
192.168.186.0/24 dev eth1 proto kernel scope link src 192.168.186.79

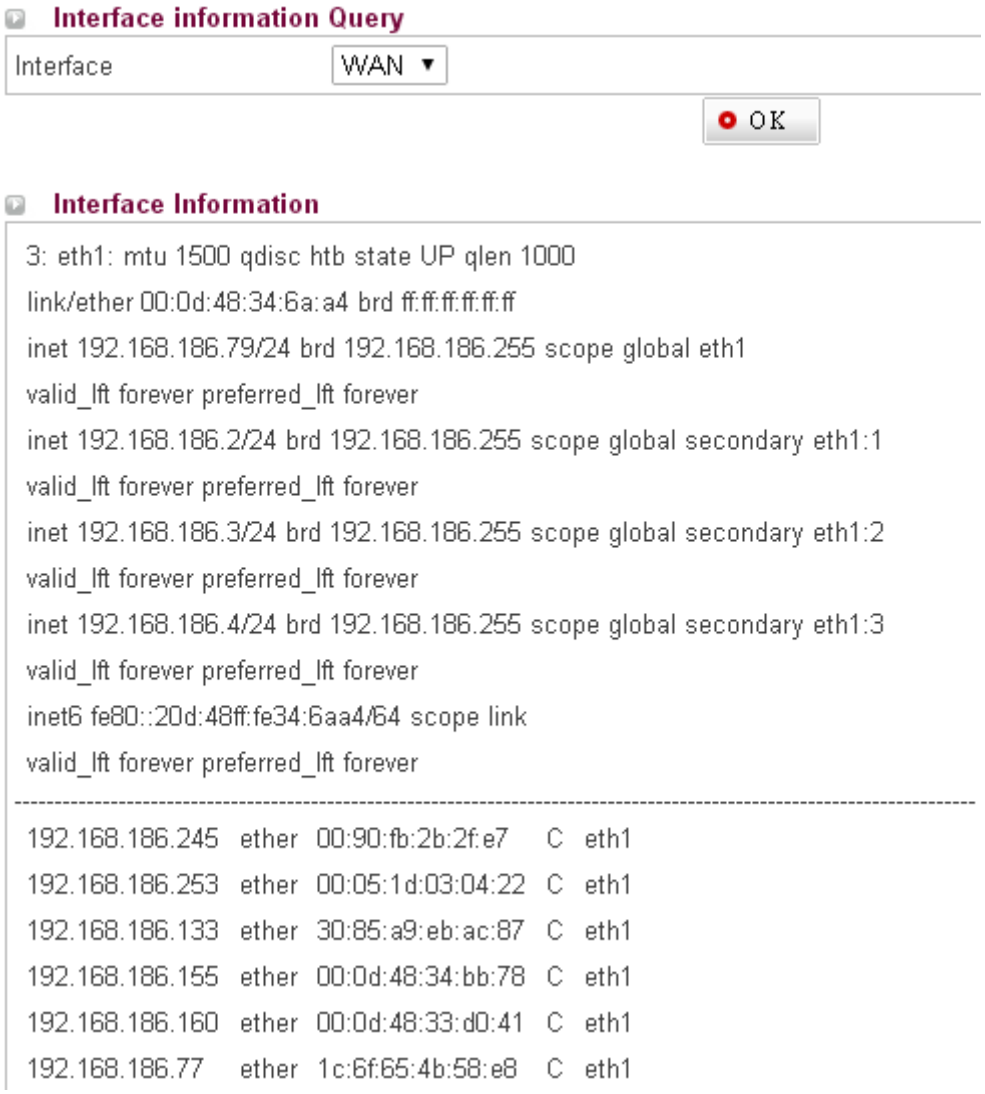
12.1.6 Interface Information

It shows the present interface information within your IFW320.

LAN information:

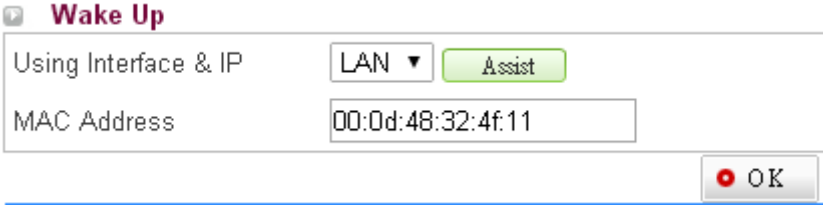

Interface information Query
Interface
LAN
OK
Interface Information
2: eth0: mtu 1500 qdisc htb state DOWN qlen 1000
link/ether 00:0d:48:34:6a:a3 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
valid_lft forever preferred_lft forever
inet 192.168.99.0/24 brd 192.168.99.255 scope global eth0:1
valid_lft forever preferred_lft forever
inet6 fe80::20d:48ff:fe34:6aa3/64 scope link
valid_lft forever preferred_lft forever
192.168.1.111 ether 40:61:86:66:fc:ff CM eth0

WAN information:


Interface information Query
Interface
WAN
OK
Interface Information
3: eth1: mtu 1500 qdisc htb state UP qlen 1000
link/ether 00:0d:48:34:6a:a4 brd ff:ff:ff:ff:ff:ff
inet 192.168.186.79/24 brd 192.168.186.255 scope global eth1
valid_lft forever preferred_lft forever
inet 192.168.186.2/24 brd 192.168.186.255 scope global secondary eth1:1
valid_lft forever preferred_lft forever
inet 192.168.186.3/24 brd 192.168.186.255 scope global secondary eth1:2
valid_lft forever preferred_lft forever
inet 192.168.186.4/24 brd 192.168.186.255 scope global secondary eth1:3
valid_lft forever preferred_lft forever
inet6 fe80::20d:48ff:fe34:6aa4/64 scope link
valid_lft forever preferred_lft forever
192.168.186.245 ether 00:90:fb:2b:2f:e7 C eth1
192.168.186.253 ether 00:05:1d:03:04:22 C eth1
192.168.186.133 ether 30:85:a9:eb:ac:87 C eth1
192.168.186.155 ether 00:0d:48:34:bb:78 C eth1
192.168.186.160 ether 00:0d:48:33:d0:41 C eth1
192.168.186.77 ether 1c:6f:65:4b:58:e8 C eth1

12.1.7 Wake Up

Click on Assist to select which IP users want to wake it up.

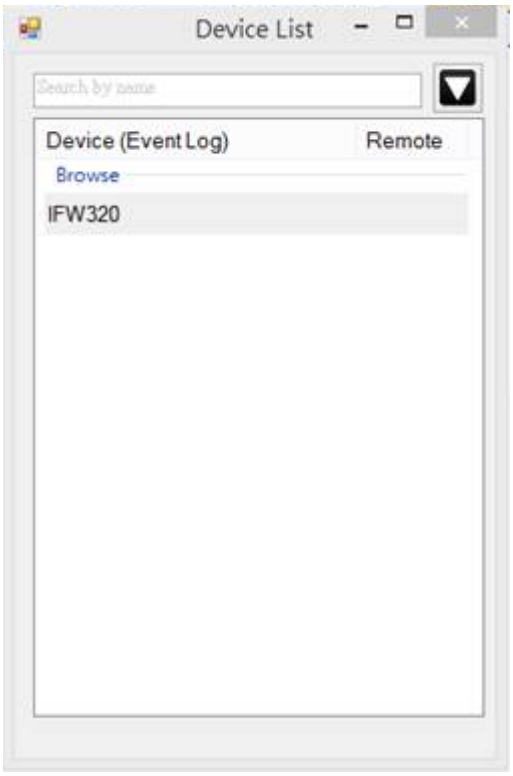


12.2 Remote Management

In this section we will show you how to implement efficient and easy remote management to IFW320 through Axiomtek AXView 2.0. This function gives you the possibility to access IFW320 management interface from a host device.

Follow the steps given below:

1. Install AXView 2.0 in a host device, then launch “Remote Manager” program to view IFW320. From figure below, you can see that IFW320 is found and added to Device List.



2. Double click on “IFW320”, and you may get a message asking whether you want to open the browser.

3. Click on “Yes” to start browser which will connect automatically to IFW320 management interface. Default HTTPS port number is 443. If you have changed the default HTTPS port number in management interface, you must add that new port number manually to the end of URL (e.g. *https://192.168.1.1:4433*, where 4433 is new port number).

This page is intentionally left blank.

Chapter 13
Logs

In this Logs chapter you can enable the following lists:

- System Operation

13.1 System Operation

Log records all connections that pass through the IFW320. The information is classified as Configuration, Networking, Policy, Object, and so on. Event log has the records of any system configurations made. Each log denotes who, when, what and where that a configuration is being modified. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions. You can see simply information in Logs. If you need more information, you could use Logs Search to search what logs you need. The result shows on Logs Search Result.

13.1.1 Logs

Select *Logs* > *System Operation* > *Logs*. It shows configurations which has been modified with illustration, describe what kinds of action has been modified, describe which IP address has ever done function path.

Logs List 1 / 8 1 GO

Time	Account	IP Address	Function Path	Action	Description
11-13 10:19:44	admin	192.168.189.244	VPN > PPTP Client > PPTP Client List	Add	Name
11-13 10:14:57	admin	192.168.189.244	VPN > PPTP Server > Account List	Add	Enabled
11-13 10:02:11	admin	192.168.189.244	VPN > IPSec Tunnel > VPN IPSec Tunnel List	Add	Enabled
11-13 09:34:07	admin	192.168.189.244	Login OK	Login	Login Successful
11-13 08:51:14	admin	192.168.189.244	Objects > Internet Auth > Local Users	Add	name
11-13 08:46:55	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 18:25:55	admin	192.168.189.244	IDP & Botnet > Botnet Setting > Operation Mode	Save	Enabled
11-12 17:57:03	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 17:37:02		192.168.186.133	Login OK	Login	Login False
11-12 17:27:54	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 16:40:33	admin	192.168.186.133	Login OK	Login	Login Successful
11-12 16:40:30		192.168.186.133	Login OK	Login	Login False
11-12 16:34:49	admin	192.168.189.244	Advanced Security > Intranet protect > ARP Spoofing Log	Search	IP Address
11-12 16:32:22	admin	192.168.189.244	Advanced Security > Switch Management	Add	Interface
11-12 16:20:44	admin	192.168.189.244	Policy > LAN Policy > LAN to WAN Policy	Add	Policy Name
11-12 16:16:50	admin	192.168.189.244	Network Services > Remote Syslog Server > Remote Connect Setup	Save	Enable

Time
It shows event time.

Account
Which account name has ever done the event.

IP Address
It shows account IP address.

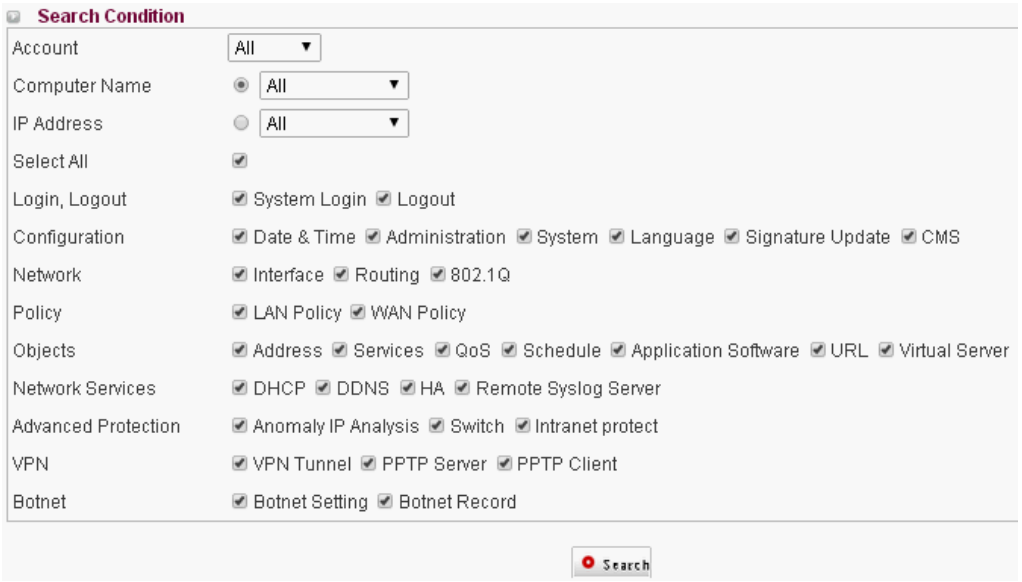
Function Path
Record the superintendent events.

Action
The superintendent carries out movement including login, add, edit, delete, search, refresh, and so on.

Description
Describe the event.

13.1.2 Logs Search

Select *Logs* > *System Operation* > *Logs Search*.



Account
Available account which administrator made before.

Computer Name
All of available computers which ever pass through the IFW320.

IP Address
Internal IP addresses.

Login, Logout
Record users login and logout action.

Configuration
It lists out the working connections for the Date&Time, Administration, System and Language logs.

Network
It lists out the working connections for the Interface and Routing logs.

Policy
It lists out the working connections for the LAN Policy and WAN Policy logs.

Objects
It lists out the working connections for the Address, Services, QoS, Schedule, Application Software, URL and Virtual Server logs.

Network Services
It lists out the working connections for the DHCP, DDNS, HA and Remote Syslog Server.

Advanced Protection
It lists out the working connections for the Anomaly IP Analysis, Switch and Intranet protect.

VPN
It lists out the working connections for the VPN Tunnel, PPTP Server and PPTP Client logs.

BotNet
It lists out the working connections for the BotNet Setting and BotNet Record.

13.1.3 Logs Search Result

Select *Logs > System Operation > Logs Search Result*.

After click on

, you will see Logs Search Result as shown in example below.

Search Result 1 / 8 1 GO

Time	Account	IP Address	Function Path	Action	Description
11-13 10:19:44	admin	192.168.189.244	VPN > PPTP Client > PPTP Client List	Add	Name
11-13 10:14:57	admin	192.168.189.244	VPN > PPTP Server > Account List	Add	Enabled
11-13 10:02:11	admin	192.168.189.244	VPN > IPSec Tunnel > VPN IPSec Tunnel List	Add	Enabled
11-13 09:34:07	admin	192.168.189.244	Login OK	Login	Login Successful
11-13 08:46:55	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 18:25:55	admin	192.168.189.244	IDP & Botnet > Botnet Setting > Operation Mode	Save	Enabled
11-12 17:57:03	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 17:37:02		192.168.186.133	Login OK	Login	Login False
11-12 17:27:54	admin	192.168.189.244	Login OK	Login	Login Successful
11-12 16:40:33	admin	192.168.186.133	Login OK	Login	Login Successful
11-12 16:40:30		192.168.186.133	Login OK	Login	Login False
11-12 16:34:49	admin	192.168.189.244	Advanced Security > Intranet protect > ARP Spoofing Log	Search	IP Address
11-12 16:32:22	admin	192.168.189.244	Advanced Security > Switch Management	Add	Interface
11-12 16:20:44	admin	192.168.189.244	Policy > LAN Policy > LAN to WAN Policy	Add	Policy Name
11-12 16:16:50	admin	192.168.189.244	Network Services > Remote Syslog Server > Remote Connect Setup	Save	Enable
11-12 16:16:46	admin	192.168.189.244	Network Services > Remote Syslog Server > Remote Connect Setup	Save	Enable

This page is intentionally left blank.

Chapter 14
Status

This function provides current information about the device and the network including addresses for LAN/WAN, subnet masks, default gateways, DNS, etc. as well as current network connection status and various other information. In this Status chapter you can enable the following lists:

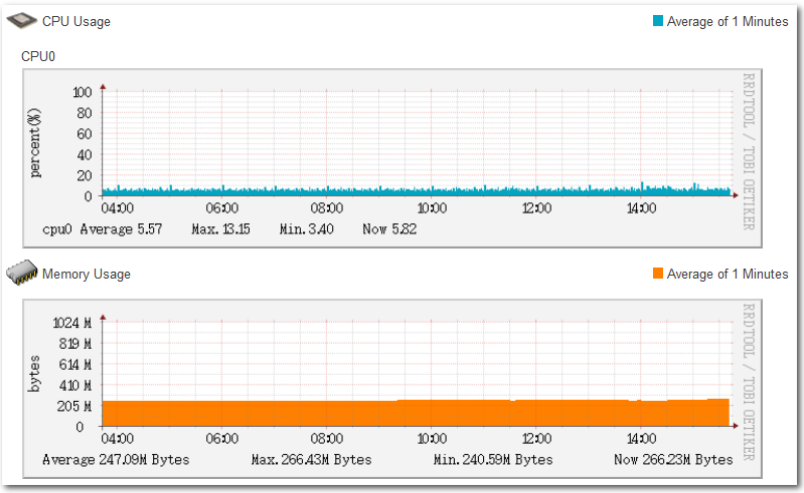
- Performance
- Connection Status
- Flow Analysis

14.1 Performance

There are three parts, System Status, Interface Flow, and History Status. Performance section shows the utilization of CPU Usage, Memory Usage and System Usage. Besides downloading each interface's current resource and flow capacity, it is also possible to inquire the historical capacity information.

14.1.1 System Status

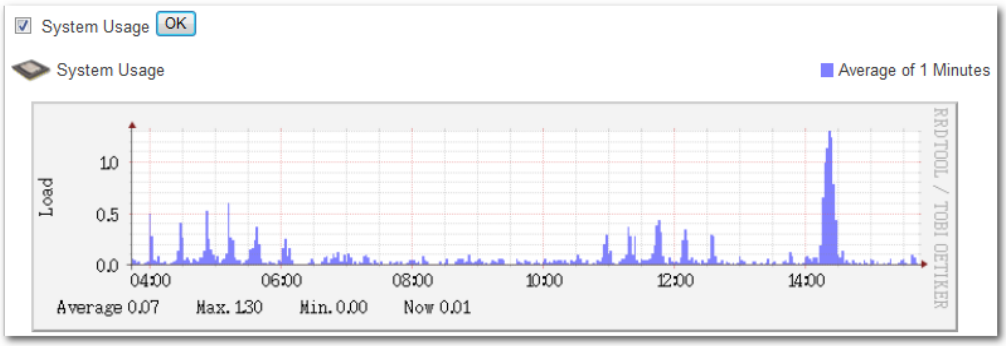
Generally speaking, system status shows graphs of resource usage. It shows last 12 hours machine status. Select *Status* > *Performance* > *System Status*. There are three graphs: CPU Usage, Memory Usage, and System Usage.



CPU Usage
The CPU utilization of the device.

Memory Usage
The Memory utilization of the device.

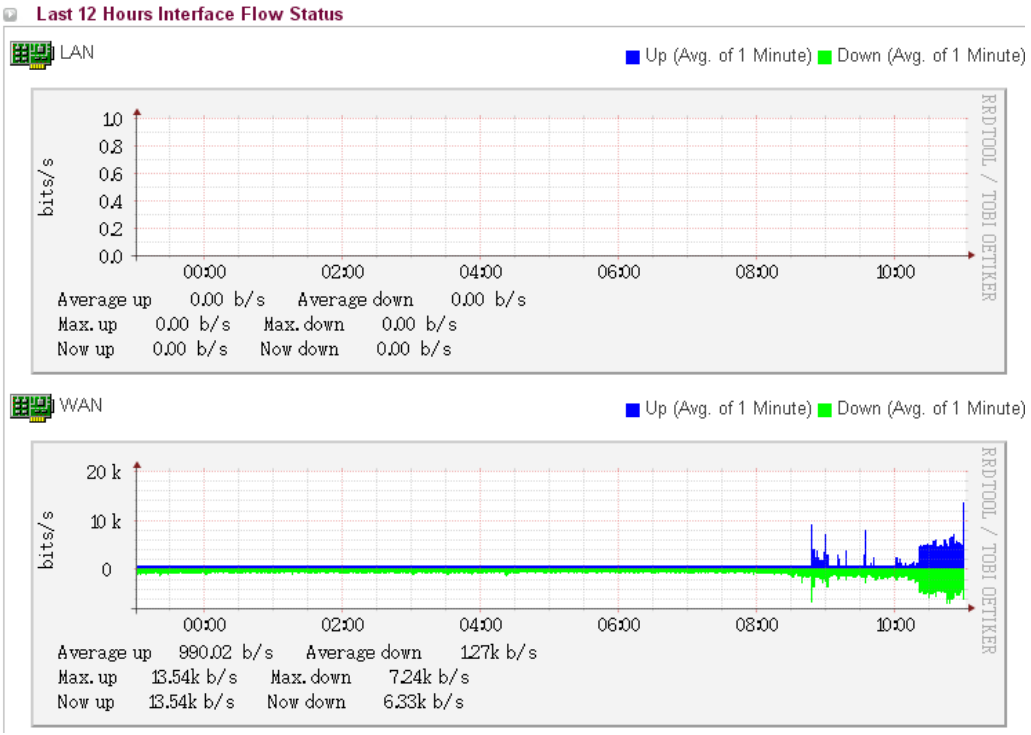
In addition, select “System Usage” tick box and click on OK, then you will get graphs of System Usage.



System Usage
The System utilization of the device.

14.1.2 Interface Flow

Select *Status* > *Performance*> *Interface Flow*. It shows graphs of incoming and outing traffic through that interface.

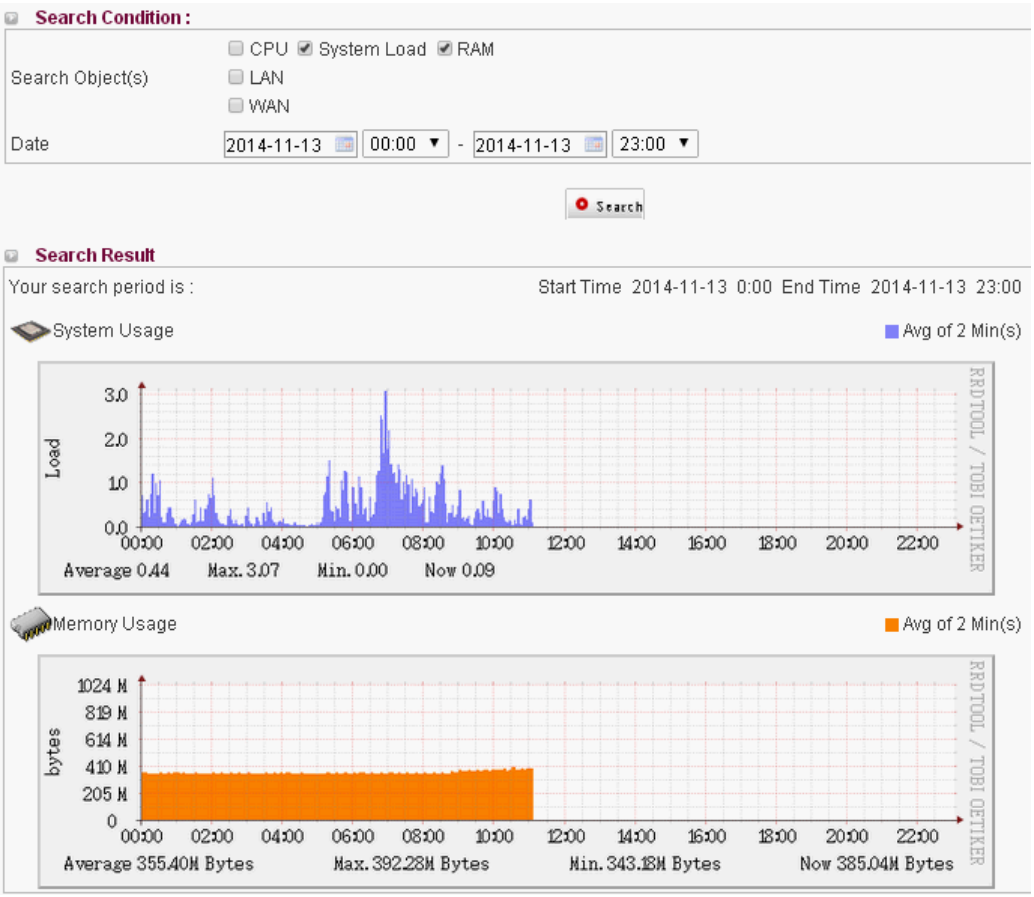


LAN
The LAN utilization of the device.

WAN
The WAN utilization of the device.

14.1.3 History Status

Select *Status* > *Performance* > *History Status*. Set information, and click on Search. Then, you will see Search Result. It shows the history system condition.



Search Object(s)
There are CPU, System Load, RAM, LAN and WAN.

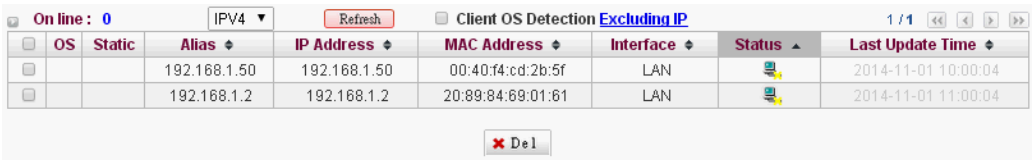
Date
Select date ranges.

14.2 Connection Status

The Connection Status section records all the connection status of host PCs that have ever connected to the IFW320. It shows computer list and connect track.

14.2.1 Computer List

Select *Status* > *Connection Status* > *Computer List*. It shows the current connection status information.



OS
User has to select Client OS Detection, and click on Refresh. It shows different OS system which those computers used.

Alias
The computer's network identification name.

IP Address
The computer's IP address.

MAC Address
The computer's network adapter identification number.

Interface
You could know where the connecter is from, LAN or BRI.

Status
1. : On-line.
2. : Off-line.

Last Update Time
Display the date and time users login (year / month / day / hour / minute / seconds).

You can click on Refresh to get the current connection status information.

14.2.2 Connection Track

According to the network packet analysis and tracing, it analyzes each of user's behavior on the Internet. This function originates the end name to take the classification, demonstrated the record of all current users containing the IP address, Session, Up speed bits, Down speed bits, and Log.

Select *Status* > *Connection Status*> *Connection Track*. It shows the upload and download flow status of all current users of the computer.

Computer Name
The computer's network identification name.

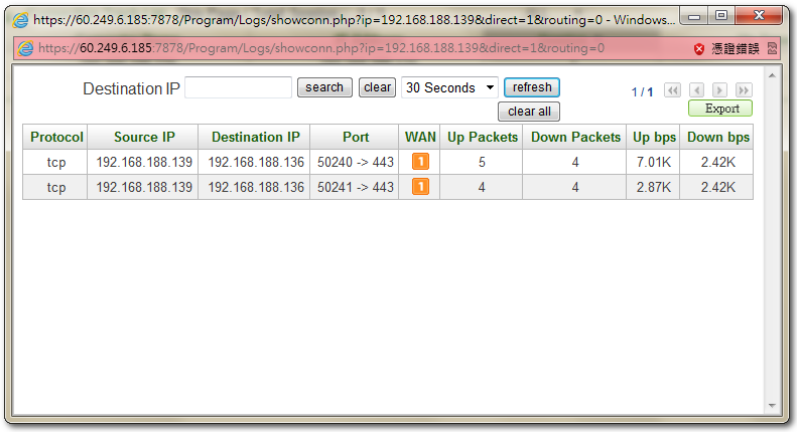
IP Address
It shows the computer IP Address.

Session
It shows the current number of sessions connected to the computer.

Up Speed bits
It shows the upstream bandwidth for the computer. Eight bits is a unit of a bytes/second. 1024 bytes = 1 KB.

Down Speed bits
It shows the downstream bandwidth for the computer. Eight bits is a unit of a bytes/second. 1024 bytes = 1 KB.

Click on Log
It shows more detail information, see figure below.



Destination IP search
Type the specific IP address you want to search.

Port
It shows the packets going through from source port to destination port.

Up Packets
It shows the current upload flows.

Down Packets
It shows the current download flows.

Up bps
The accumulation of upload flow. Eight bits is a unit of a bytes/second. 1024 bytes = 1 KB.

Down bps
The accumulation of download flow. Eight bits is a unit of a bytes/second. 1024 bytes = 1 KB.

14.3 Flow Analysis

It shows all main flow of connection. This function not only records the Downstream Flow and Up Flow, but also provides the IT administrator with detailed statistical reports and charts. In this section, it shows Top Flow List, Top Flow List by Port, and Top Flow Search.

14.3.1 Top N Flow

Select *Status* > *Flow Analysis* > *Top N Flow*.

Flow Direction
There are two selections. Default setting is OutBound.
1. Outgoing.
2. Incoming.

Top N Flow
Select how many lists would be shown. Default setting is 10.

Computer Name
The computer's network identification name.

IP Address
It shows the computer IP Address.

MAC Address
The computer's network adapter identification number.

Up Flow(kbytes)
The accumulation of upload flows. 1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

Down Flow(kbytes)
The accumulation of download flows. 1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

If you want to know which service port the IP address is connecting to, select the rectangular form to show Top N Flow details. Then, you will see a figure as given below.

IP : 192.168.5.34 Type : Outgoing

Service	Up Flow(kbytes)	Percentage	Down Flow(kbytes)	Percentage	Record
FTP	1,011.40	3%	1,493.16	< 1%	Log
DNS	1.12	< 1%	3.18	< 1%	Log
HTTP	5,047.43	14%	92,152.68	25%	Log
HTTPS	5,322.36	15%	16,945.72	5%	Log
other	24,773.51	69%	257,228.50	70%	Log

Click on Log to see Top N Flow Log in figure below.

IP : 192.168.5.34 Type : Outgoing Service : FTP Reverse Dst IP Back 1 / 9 1 GO Export

Date	Protocol	Src IP	Dst IP	Port	WAN	Up Flow(kbytes)	Down Flow(kbytes)	Policy
2013-09-24 08:03:44	tcp	192.168.5.34	163.29.242.28	49279 -> 21	1	5.50	8.17	
2013-09-24 08:06:54	tcp	192.168.5.34	163.29.242.28	49459 -> 21	1	5.55	8.30	
2013-09-24 08:10:03	tcp	192.168.5.34	163.29.242.28	49592 -> 21	1	5.50	8.18	
2013-09-24 08:11:39	tcp	192.168.5.34	163.29.242.29	49624 -> 21	1	2.28	3.16	
2013-09-24 08:13:20	tcp	192.168.5.34	163.29.242.28	49651 -> 21	1	5.50	8.17	
2013-09-24 08:13:41	tcp	192.168.5.34	163.29.242.29	49686 -> 21	1	2.01	2.76	
2013-09-24 08:16:12	tcp	192.168.5.34	163.29.242.29	49758 -> 21	1	16.26	22.31	
2013-09-24 08:16:33	tcp	192.168.5.34	163.29.242.28	49807 -> 21	1	5.50	8.18	
2013-09-24 08:19:44	tcp	192.168.5.34	163.29.242.28	49851 -> 21	1	6.29	9.16	
2013-09-24 08:23:07	tcp	192.168.5.34	163.29.242.28	49898 -> 21	1	5.55	8.26	
2013-09-24 08:26:27	tcp	192.168.5.34	163.29.242.28	49947 -> 21	1	5.60	8.35	
2013-09-24 08:29:37	tcp	192.168.5.34	163.29.242.28	49998 -> 21	1	5.46	8.18	
2013-09-24 08:32:55	tcp	192.168.5.34	163.29.242.28	50151 -> 21	1	5.50	8.17	
2013-09-24 08:36:04	tcp	192.168.5.34	163.29.242.28	50405 -> 21	1	5.50	8.18	
2013-09-24 08:39:17	tcp	192.168.5.34	163.29.242.28	50615 -> 21	1	5.50	8.17	

14.3.2 Top N Port Flow

Select *Status* > *Flow Analysis* > *Top N Port Flow*.

Top N Flow Search :

Flow Direction: Outgoing

Top N Flow: 10

Statistics Period: 2013-09-24 00:00:00 ~ 2013-09-24 18:32:24

Search

1 / 2 1 GO

No.	Destination Port	Up Flow	Down Flow
1	HTTP	163,292.30	1,168,952.98
2	SMTP	86,270.18	67,086.47
3	HTTPS	45,669.06	282,397.49
4	1935	2,501.09	136,854.75

Flow Direction
There are two selections. Default setting is OutBound.
1. Outgoing.
2. Incoming.

Top N Flow
Select how many lists would be shown. Default setting is 10.

Click on Search
And you will see result below.

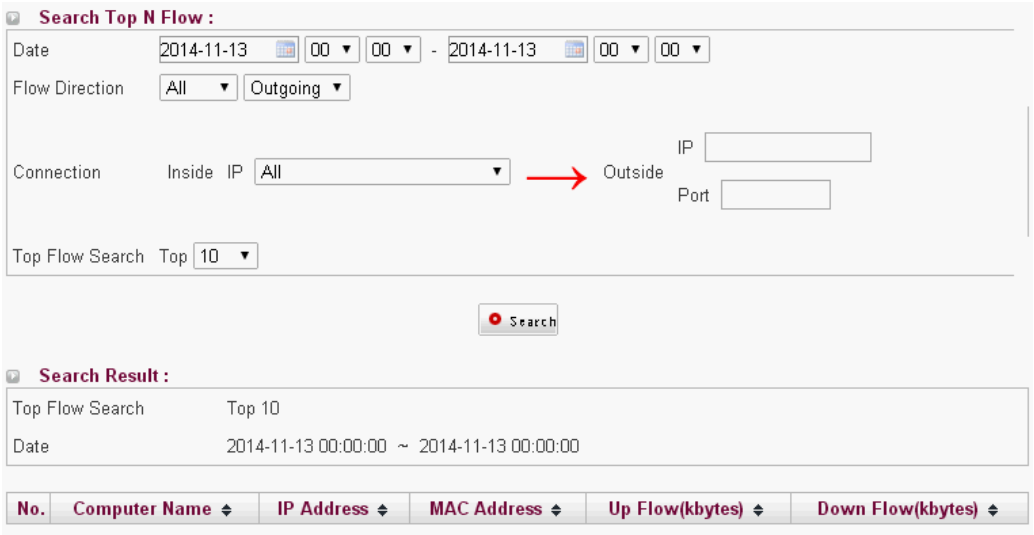
Destination Port
It shows destination port.

Up Flow
The accumulation of upload flows. 1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

Down Flow
The accumulation of download flows. 1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

14.3.3 Top N Search

Select *Status* > *Flow Analysis* > *Top N Search*.



Date
Select date range.

Flow Direction
There are two selections. Default setting is Outgoing.
1. Outgoing.
2. InComing.

Connection
Select the computer IP Address.

Top Flow Search
Select how many lists would be shown. Default setting is 10.

Click on Search
And you will see search result.

If you want to know which service port the IP address is connecting to, select the rectangular form to show Top N Search details. Then, you will see a figure as given below.

IP : 192.168.5.34 Type : Outgoing

Service	Up Flow(kbytes)	Percentage	Down Flow(kbytes)	Percentage	Record
FTP	1,011.40	3%	1,493.16	< 1%	Log
DNS	1.12	< 1%	3.18	< 1%	Log
HTTP	5,047.43	14%	92,152.68	25%	Log
HTTPS	5,322.36	15%	16,945.72	5%	Log
other	24,773.51	69%	257,228.50	70%	Log